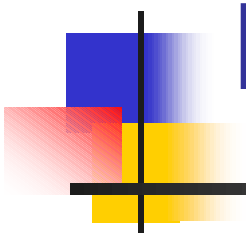
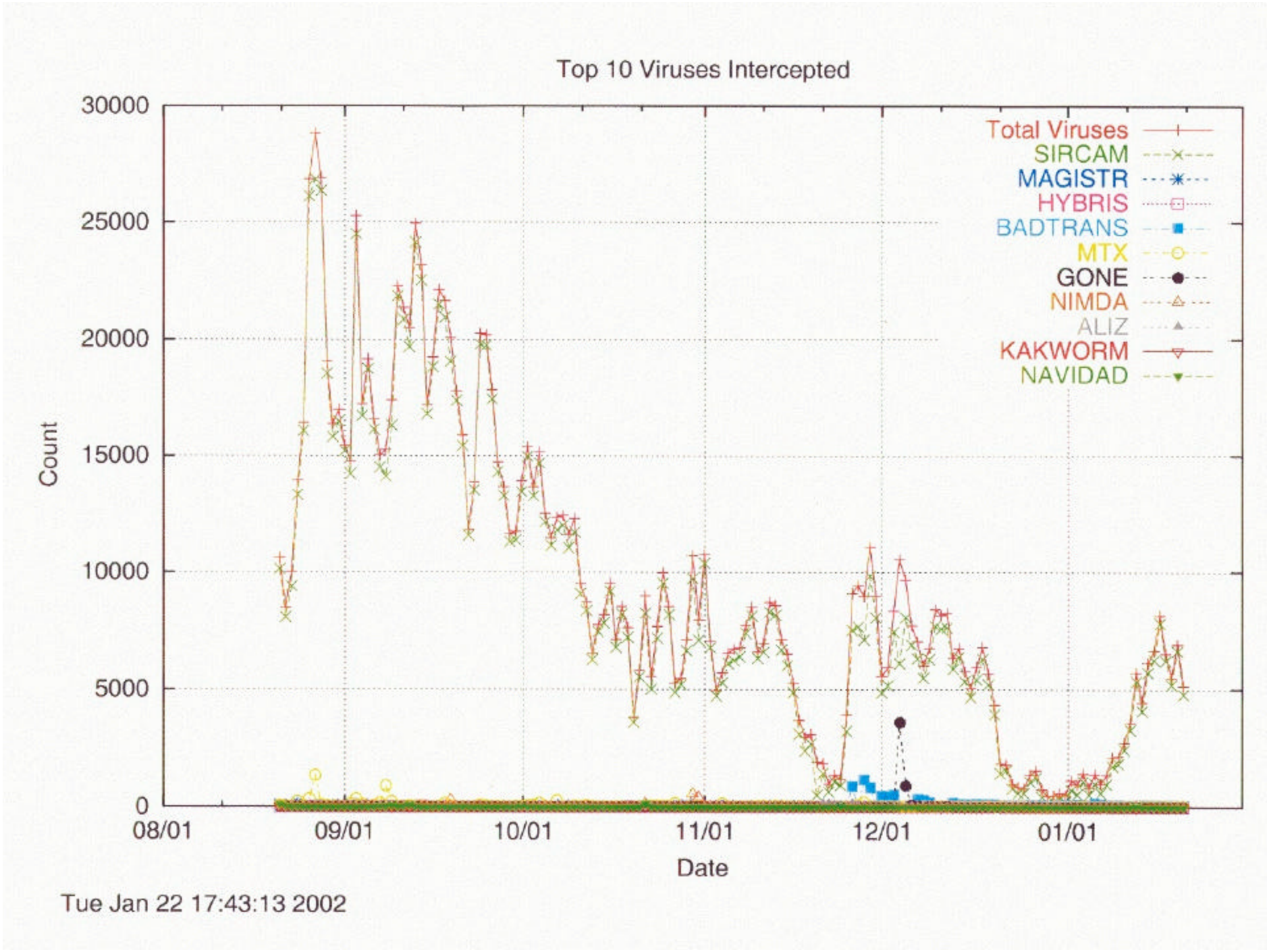
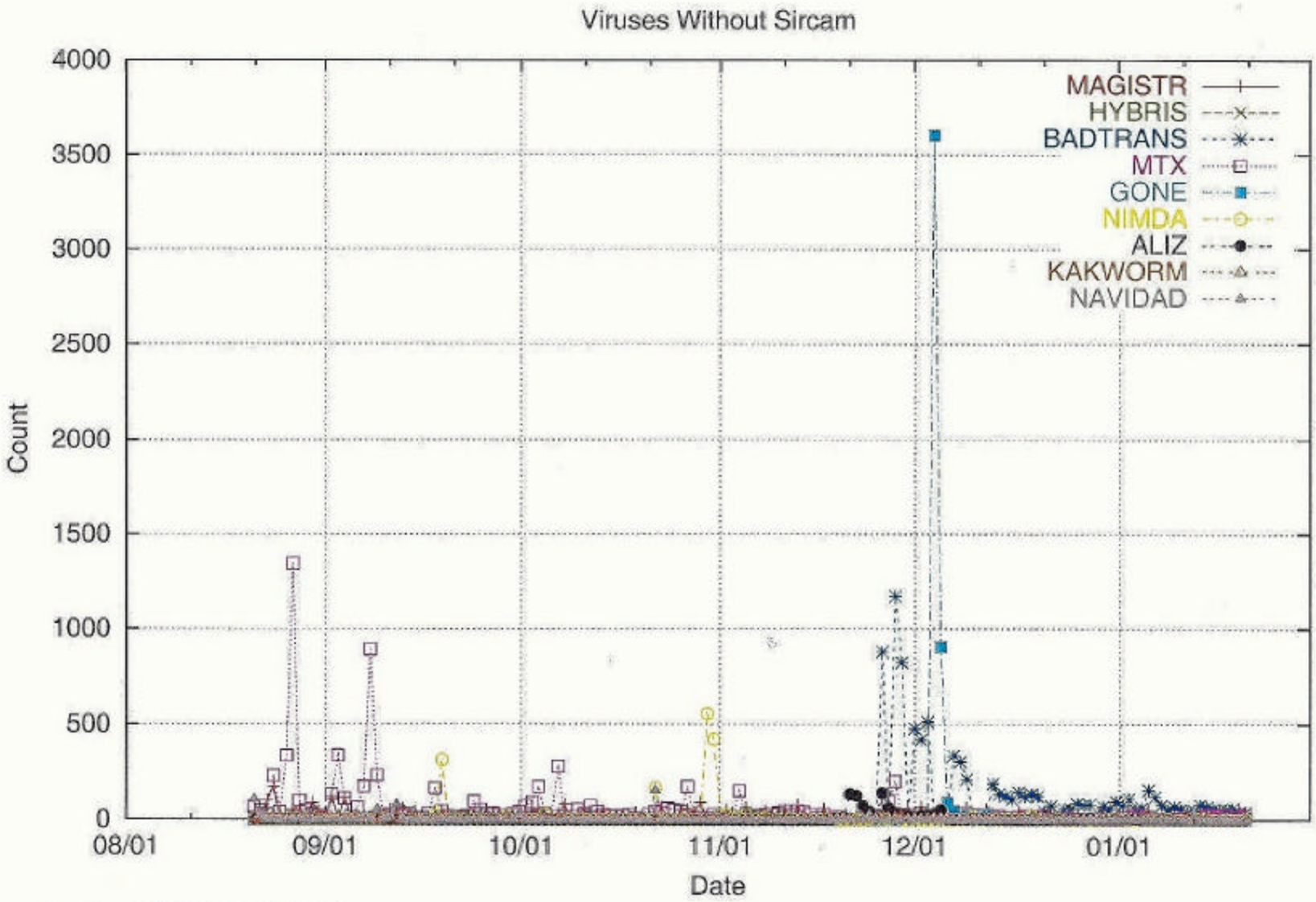


Security in a University Environment

Randy Marchany
VA Tech Computing Center
Blacksburg, VA 24060
Marchany@vt.edu


Top 10 Viruses Intercepted
Total Viruses
SIRCAM
MAGISTR
HYBRIS
BADTRANS
MTX
GONE
NIMDA
ALIZ
KAKWORM
NAVIDAD
Count
30000
25000
20000
15000
10000
5000
0
08/01
09/01
10/01
11/01
12/01
01/01
Date
Tue Jan 22 17:43:13 2002


Viruses Without Sircam
4000
3500
3000
2500
2000
1500
1000
500
0
Count
08/01
09/01
10/01
11/01
12/01
01/01
Date
MAGISTR
HYBRIS
BADTRANS
MTX
GONE
NIMDA
ALIZ
KAKWORM
NAVIDAD
Tue Jan 22 17:43:13 2002

Instant Macro-Virus Maker (IMVM) - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

The Instant Macro-Virus Maker (IMVM) v1.2

This, as far as I know, is the first (and only) on-line virus creation tool.
NO DOWNLOAD, NO WASTED TIME, NO PROGRAMING SKILL NEEDED!!!
Choose from the options (few, I know, but it's the first edition) and then copy/paste the generated code into a Word (97...2000 etc.) module named after the virus. Enjoy!!!

Virus name:

Name

Author's name:

Your name

Used macro:

AutoOpen

Text to display:

A text to show

The date when the text is shown (between 1 and 31):

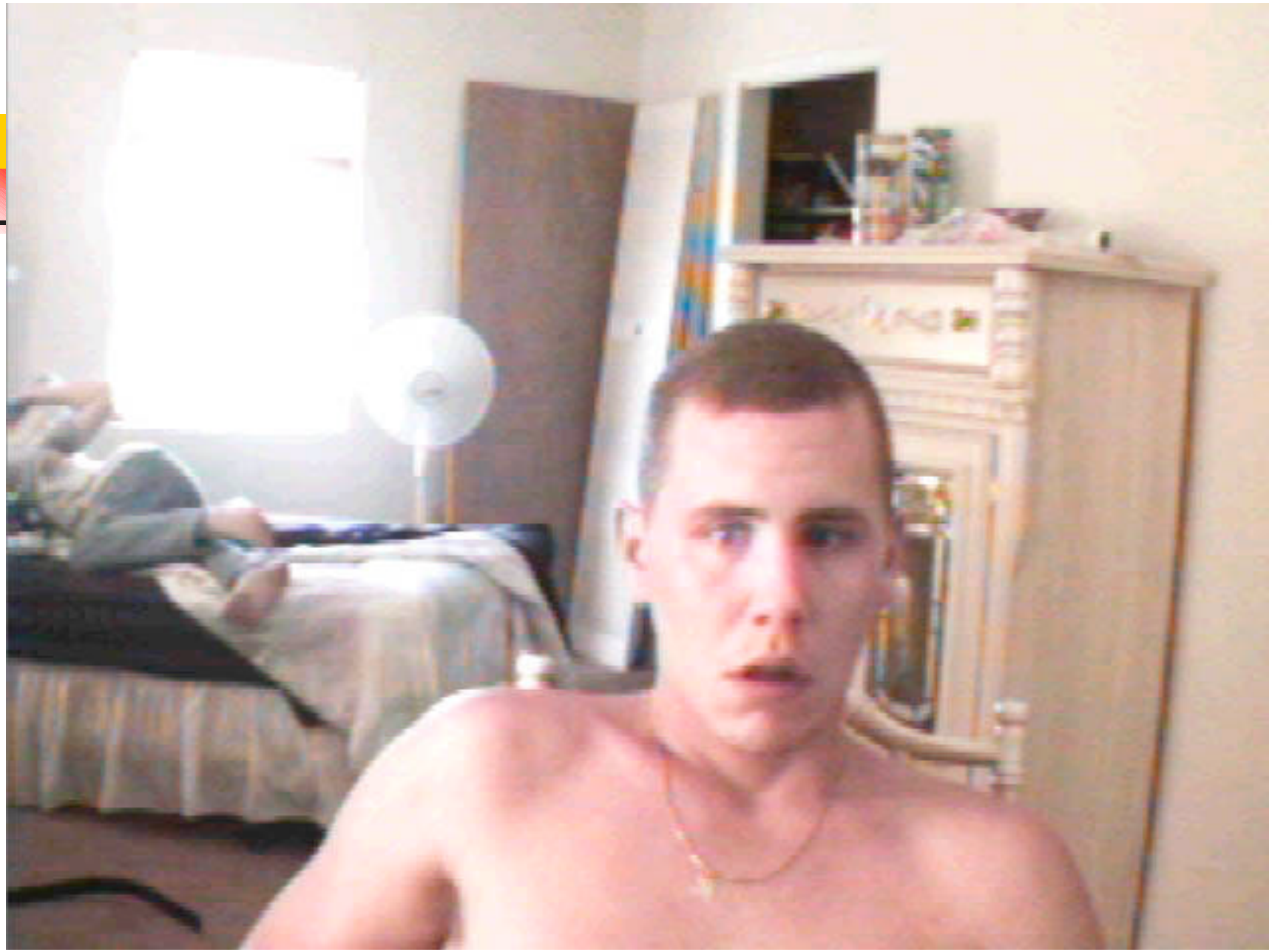
00

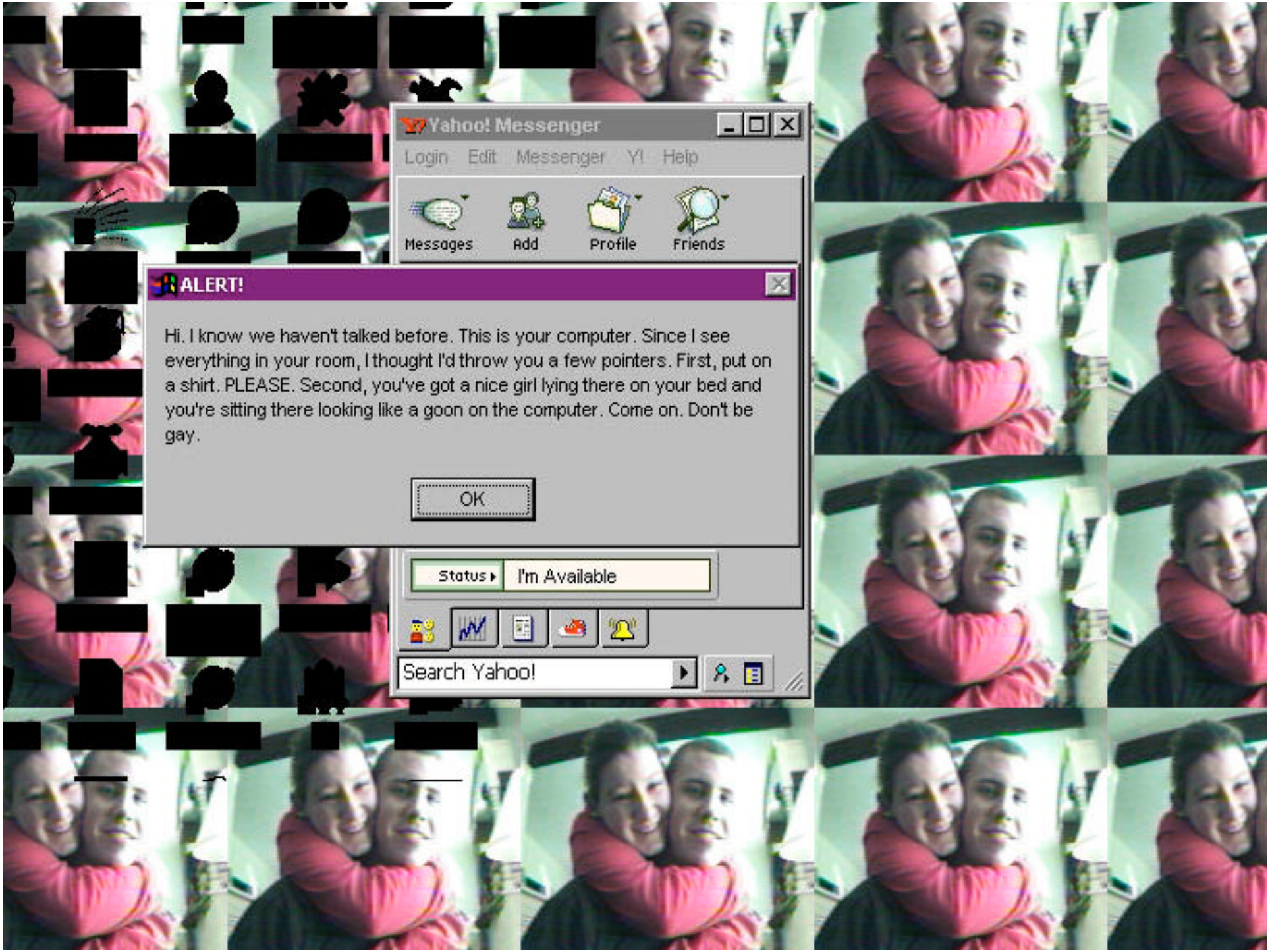
Generate

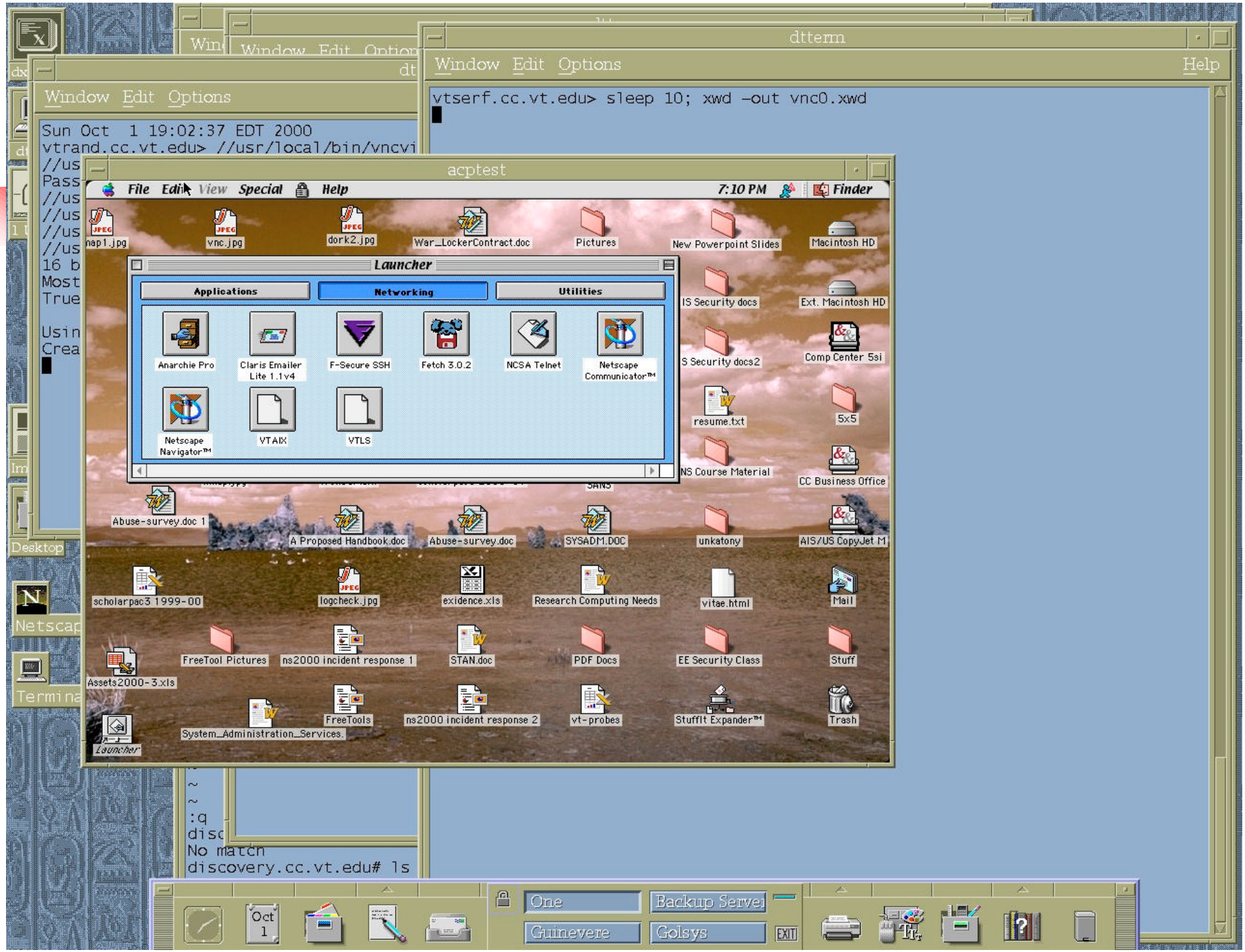
Final source:

Document: Done

Start | Insta... | vtran... | World'... | Today... | Get M... | Amazi... | 5:46 PM




Yahoo! Messenger
Login Edit Messenger Y! Help
Messages
Add
Profile
Friends
ALERT!
Hi. I know we haven't talked before. This is your computer. Since I see everything in your room, I thought I'd throw you a few pointers. First, put on a shirt. PLEASE. Second, you've got a nice girl lying there on your bed and you're sitting there looking like a goon on the computer. Come on. Don't be gay.
OK
Status
I'm Available
Search Yahoo!

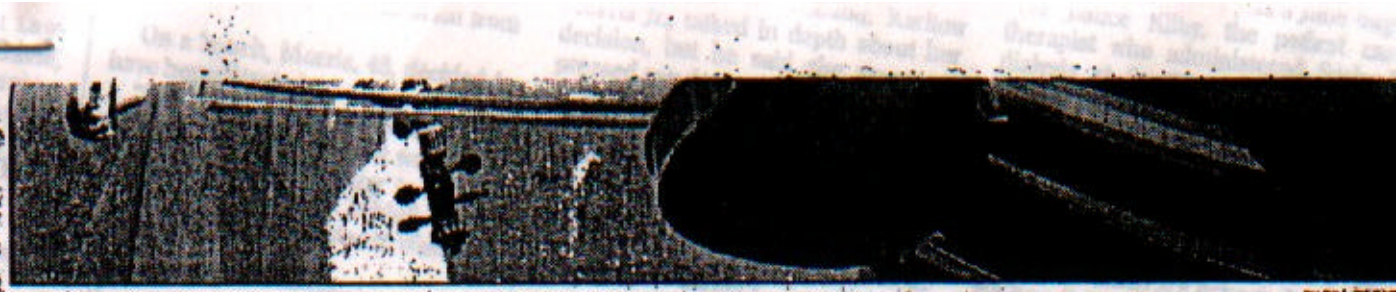

dtterm
Window Edit Options
Help
vtserf.cc.vt.edu> sleep 10; xwd -out vnc0.xwd
dt
Window Edit Options
Sun Oct 1 19:02:37 EDT 2000
vtrand.cc.vt.edu> //usr/local/bin/vncvi
acptest
File Edit View Special Help
7:10 PM
Finder
Launcher
Applications
Networking
Utilities
Anarchie Pro
Claris Emailer Lite 1.1v4
F-Secure SSH
Fetch 3.0.2
NCSA Telnet
Netscape Communicator™
Netscape Navigator™
VTAIX
VTLS
nap1.jpg
vnc.jpg
dork2.jpg
War_LockerContract.doc
Pictures
New Powerpoint Slides
Macintosh HD
IS Security docs
Ext. Macintosh HD
S Security docs2
Comp Center 5si
resume.txt
5x5
NS Course Material
CC Business Office
Abuse-survey.doc 1
A Proposed Handbook.doc
Abuse-survey.doc
SYSADM.DOC
unkatony
AIS/US CopyJet M1
scholarpac3 1999-00
logcheck.jpg
exidence.xls
Research Computing Needs
vitae.html
Mail
FreeTool Pictures
ns2000 incident response 1
STAN.doc
PDF Docs
EE Security Class
Stuff
Assets2000-3.xls
FreeTools
ns2000 incident response 2
vt-probes
StuffIt Expander™
Trash
System_Administration_Services.
Launcher
No match
discovery.cc.vt.edu# ls
Oct 1
One
Backup Server
Guinevere
Golsys
EXIT


2 Unseen
dtterm
Window Edit Options
Help
locutus
My Documents
RealPlayer Basic
vncviewer
BNChange_...
unkatony
Schulz
JCSC
sans1
My Computer
Aladdin Expander 5.0
w3i2
vnc_x86_wi...
Draft_Agen...
My Network Places
Microsoft Outlook
IDandPF-Ja...
B&N - Change Managment...
assetwt
Recycle Bin
vt-probes
SANS
unit1 ir2
fsisac1
RA-Dept01-...
web2
SANS2001 Audit
SANS2001 FreewareTools
Internet Explorer
SSH Secure Shell Client
WS_FTP
vwm
EE Class
assetrisk
cacert
SANS2001 IR
03
ranum
beta
Powerpoint Presentations
FreewareTools
Acrobat Reader 4.0
Conference Papers
Netscape Communicator
Take5
VT.Site.qte
univ
uva
AOL Instant Messeng...
cc32d476
AAA
Email
CIS Rulers
Security_Ar...
Stuff
Start
Microsoft PowerPoint - [u...
1:47 PM
ame <name>] [-
100235 1 tcp 3
vtserf.cc.vt.edu> sleep 5; xwd -out w2kvnc.xwd
Apr 25
dxconsc
dtterm
dtterm
Desktop
ImageVi
ImageVi
Netscap
Netsc
Terminal

on you.
who've
om,
laced up in
betrayed.
ust for my
ng parents,
tradition
the youths
no've had
he law,
evaporate
c on court.
y like how
crisy in older

y, criticizing
ect how
gh your
to abandon

the two most
yers in the
stories
nt realities of
s had every
es it, refusing
or his family.
harder
kids relate
d hard and
ol. 1



Elvis Vidal, left, watches Tis Adams for cues before a performance yesterday's outdoor event to celebrate a commitment near the Good Shepherd Music Center in Adams-Morgan. The center, businesses to help renovate the center. The program a housed in the basement of the Ontario Court apartments, sponsored children build self-esteem as they develop music skills

Hackers Breach GMU Computers, Zap Students'

By Ann O'Hanlon
Washington Post Staff Writer

Hackers have broken into computers at George Mason University 12 times since February, and in the most recent incident, they deleted academic work for 400 computer and engineering students, authorities said.

Campus and Fairfax County police are investigating the incidents, and they have filed charges against two students in connection with a February break-in.

Much of the information lost in the latest, and most serious, attack—which occurred three weeks ago—was recovered from backup systems. But because the most recent backup of data had been done a month earlier, many students lost extensive work they had performed over the summer, faculty members said.

Three master's degree candidates working with George Mason professor Jeff Offutt could not recover any of their semester projects.

"A lot of people are very upset, because it's been a major loss of work and a major annoyance," Offutt said.

"One person came into my office crying. . . . She was saying, 'Please, it wasn't my fault. It wasn't my fault. It was working. You can ask my friends who saw it.' She just kept saying it over and over. I felt so sorry for her."

Attacks by computer vandals are nearly as old as computing, but experts say such incidents may be growing more common and more malicious.

"We are seein
crease," said Ch
founder of Inter
tems in Atlanta,
accounts for abo
He attributed th
number of peop
the . . . tools th
more available to

George Mas
working to impr
system but are o
work and had fai

See GMU,

Two Sue GMU for $4.5 Million

Men Say They Were Falsely Accused in Computer Hacking Probe

- ERICA BESHEARS
shington Post Staff Writer

An alumnus and a current stu-nt who say they were falsely cused of hacking into the comput-system at George Mason Univer-y have filed a $4.5 million lawsuit ainst the school for defamation of aracter and false imprisonment.

An attorney for Robert Shvern, of Fairfax County, and Ryan elan, 25, of Centreville, said the men suffered great embarrass-nt and damage to their reputa-s and lost jobs and money as ult of charges filed against them summer, which were later pped.

hvern, who graduated with a ree in computer science in 1996, Whelan, a student since 1991, the lawsuit in Fairfax County uit Court on Aug. 5, naming the ersity and eight of its officials efendants. The suit claims the ersity violated their civil rights acted without probable cause n it investigated them.

The plaintiffs believe the prose-n was instigated out of malice without a legal and factual basis hat they suffered damages as a t of it," said Chanda L. Kinsey, ney for Shvern and Whelan.

nsey said an employer with-a job offer to Shvern after reading accounts of the charges in local newspapers, forcing Shvern to accept a job with less pay. Whelan owns a computer business called Two Radical Technologies, which also is named as a plaintiff in the suit. Kinsey said Whelan lost several clients after the charges were filed.

The lawsuit states that the university used an unproven computer audit system to identify the culprit in a February 1997 hacking incident, and that the audit was carried out by a university official—Donald Desrosiers—who had a personal dispute with Shvern.

Shvern and Whelan also allege that the university police department arrested them without probable cause, knowing that the audit would not stand up in court.

University officials said they would not comment on pending legal action.

Between February and August of last year, George Mason University suffered 12 computer break-ins by hackers.

In the first incident, hackers inserted a program into the school's computer system that sent derogatory e-mail messages about the chairman of the Computer Science Department and the school's Security Review Panel to administrative committees under the names of random students and staff members. Another break-in last summer deleted academic work for 400 computer and engineering students.

Shvern and Whelan were arrested in July 1997 in connection with the first incident. Shvern was charged with altering computer data, a felony; with willfully using a computer network without authority; and with causing a computer to malfunction. Whelan was charged with being an accessory to the crime.

The lawsuit claims that university officials in their public statements intended to falsely incriminate Shvern and Whelan in the incident that deleted students' academic work.

Charges against Shvern were dismissed at a preliminary hearing in March when a judge ruled that the evidence was insufficient to refer the case to a grand jury. Whelan's charge was dropped a month later.

No one else has been charged in connection with any of the hacking incidents, officials said.

George Mason University has worked since last year to bolster security of its computer system by creating a committee to develop new policies, spokesman Dan Walsch said.

CRIME & JUSTIC

Man Arrested in Alexandria Ca

A 27-year-old Emporia, Va., man has been ar California in connection with a December carja which a police officer and a motorist were s officials said yesterday.

Eddie O. Lee was arrested about 6 p.m. Mo rooming house by members of the FBI's Fugi warrant charging him with the carjacking, offici

On Dec. 26, an Alexandria officer tried to person at the corner of Montrose Avenue an scuffle ensued, and there was an exchange of After shooting the officer in the hand an approached a vehicle, shot the driver in the sh out of her car, officials said. The gunman fled in At the intersection of Jefferson Davis Highway he threatened another motorist and took his veh

Lee is being held in Los Angeles pending an e the carjacking charge. Lee is also wanted on firearms charges in Emporia.

Leesburg Woman Arrested in P

A 51-year-old Leesburg woman has been cha wounding after she told officers she spiked her r bug spray, police said yesterday.

Minnie Bell Hensley, of Adams Drive NE, wa and released on a $5,000 personal recognizance b

Francis Fewell, 55, who shares the home Hensley, opened the soda about 4 a.m. Aug. 10 some, put it back in the refrigerator, Leesburg p took a sip of the soda and noticed a "strange o criminal complaint filed in Loudoun County Gene

"After she drank it, she became ill and nauseou the contents of the can had been tampered with, spokesman, Capt. Clagett Moxley, said.

Fewell brought the can to the police station Moxley said. Hensley, brought in for questioning, she put bug spray in the drink to make Fewell ill documents. Police declined to comment on a Neither Fewell or Hensley could be reached for co

Partly sunny and warm
Highs: 70°-75°
Lows: 45°-50°

TOMORROW
Chance of showers
Highs: 65°-70°
Lows: 35°-40°

COLLEGIATE TIMES

97th Year, No. 44 • Blacksburg, Virginia • Friday, November 3, 2000

An independent student-run newspaper serving the Virginia Tech community since 1903

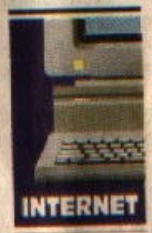
Tech computer used in Yankees hacking

by **Brian McNeill**
News Editor

A Virginia Tech computer was used in the hacking of the New York Yankees' website during the World Series last week, authorities said.

"A machine in the electrical engineering department was compromised by someone and was used in the Yankees hack," said Randy Marchany, a computer systems engineer and member of the computer incident response team, which handles online security for the university.

The hackers changed the Yankees.com numerical web address so online traffic would



the electrical engineering department, Marchany said.

Surfers expecting to see the Yankees' website were then greeted with pornographic pictures and the message "Yankees suck."

The FBI's New York office is looking into the crime.

"We are still investigating the hack of the Yankees' website," said Jim Margolin, special agent of the New York office of the FBI.

However, specific details of the investigation could not be disclosed until more developments unfold in the case, Margolin said.

"Since the investigation is ongoing, I can't say whether we have any strong leads or if there are any suspects," he said.

Marchany said he expects the hackers will most likely be caught in the near future.

"The FBI has a lot of evidence and we have a lot of evidence," he said. "We were very fast in containing the problem once we were notified of it."

Yankees.com notified Tech of the hack after their online security determined the connection to the electrical engineering computer, Marchany said.

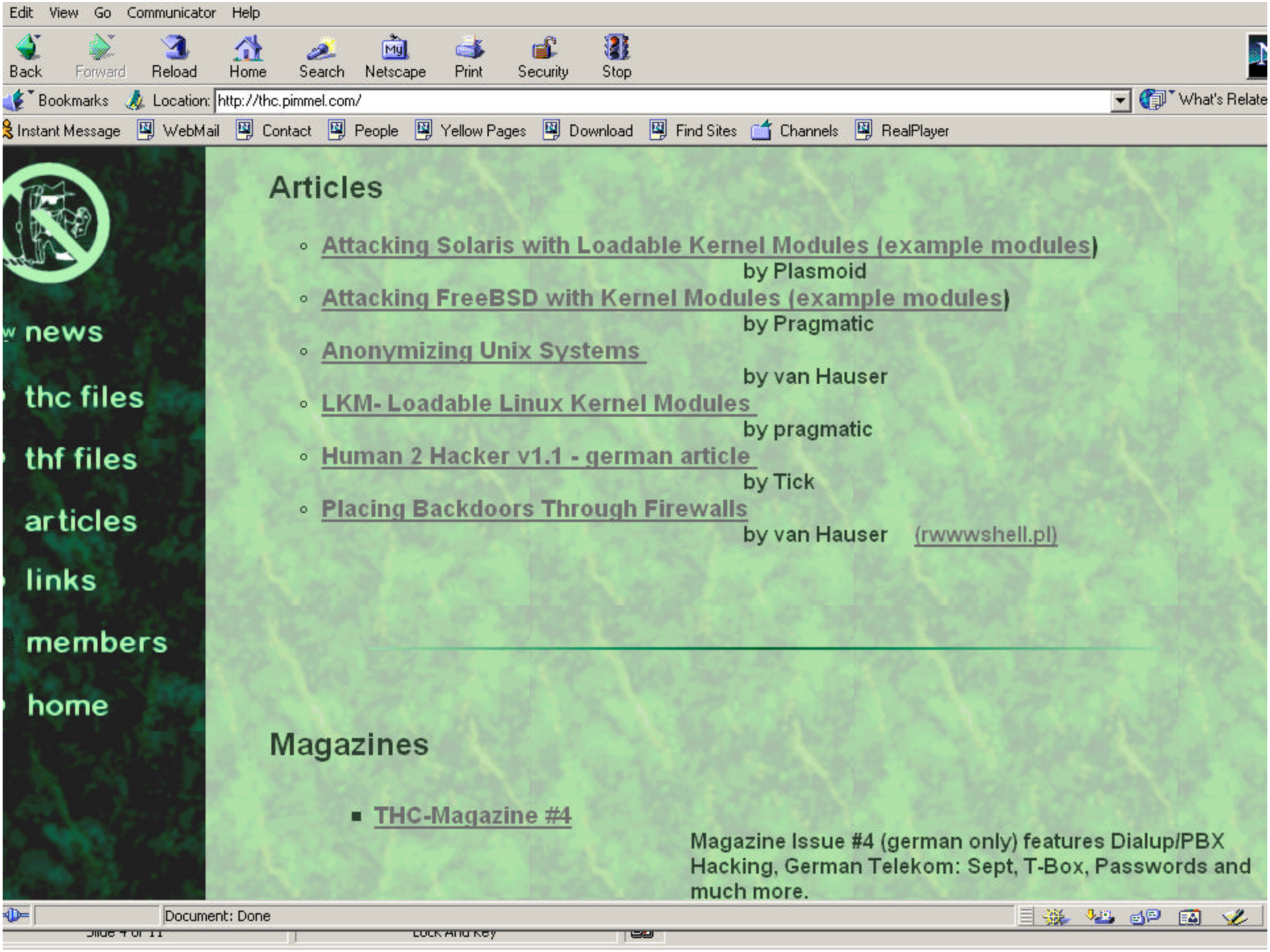
The hackers do not necessarily have any connection to Tech, Marchany said, because the attack could have been perpetrated from anywhere. Hackers search the entire Internet to locate computer weaknesses they can exploit, he said.

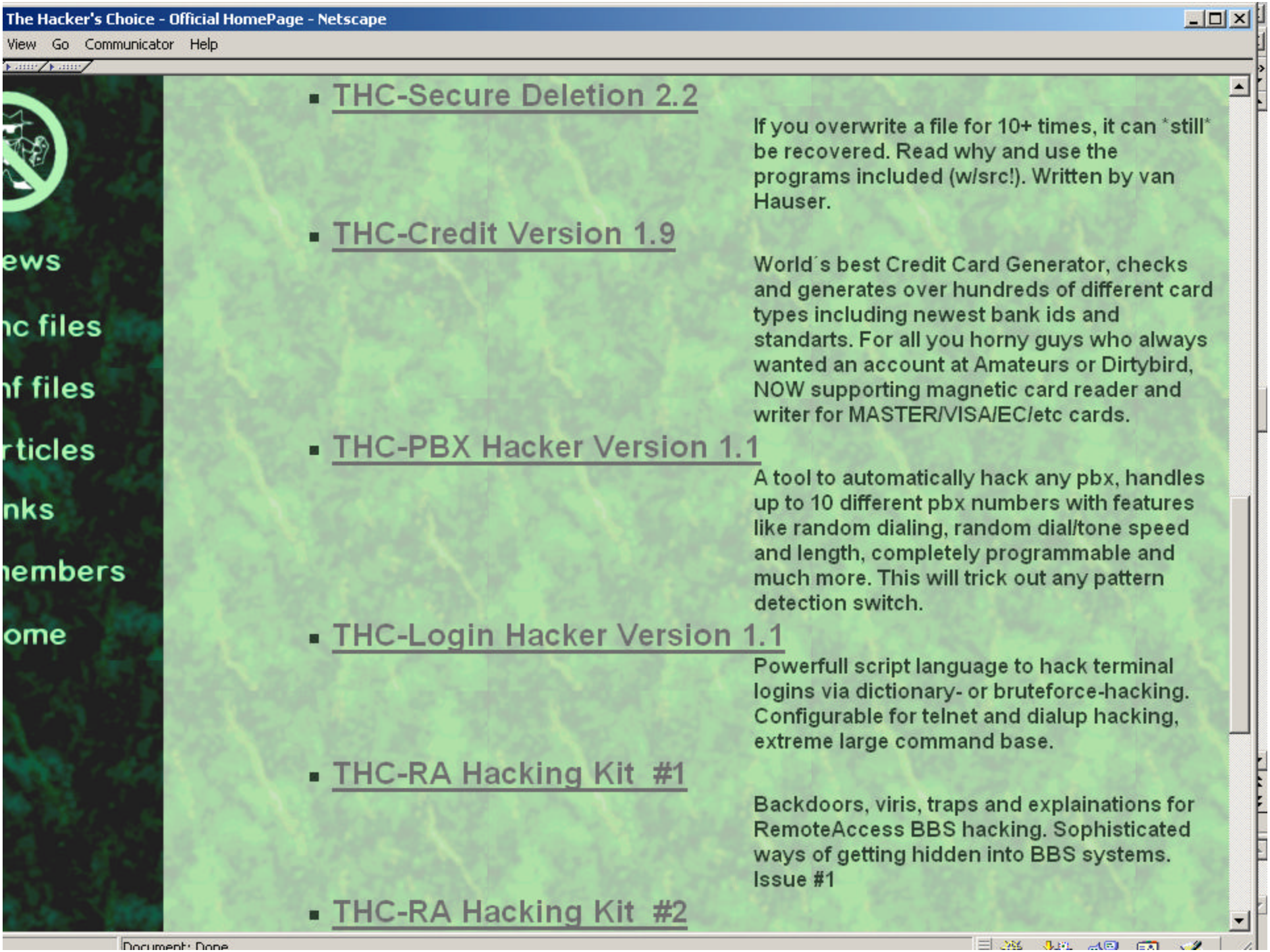
"I think there are people that regularly scan the entire Internet for vulnerable machines," he said. "It's almost as if you were to try to open the door to every home in Blacksburg, document the results and go back later and break in."

Tech has had its share of computer attacks over the years, but the computer incident response team has always quickly solved the situations, Marchany said.

"In the past 10 years, there have been probably five major attacks," he said. "We've been very good about isolating and correcting the problems."


STOP


Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://thc.pimmel.com/
What's Relate
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels RealPlayer
news
thc files
thf files
articles
links
members
home
Articles
Attacking Solaris with Loadable Kernel Modules (example modules)
by Plasmoid
Attacking FreeBSD with Kernel Modules (example modules)
by Pragmatic
Anonymizing Unix Systems
by van Hauser
LKM- Loadable Linux Kernel Modules
by pragmatic
Human 2 Hacker v1.1 - german article
by Tick
Placing Backdoors Through Firewalls
by van Hauser (rwwwshell.pl)
Magazines
THC-Magazine #4
Magazine Issue #4 (german only) features Dialup/PBX Hacking, German Telekom: Sept, T-Box, Passwords and much more.
Document: Done


The Hacker's Choice - Official HomePage - Netscape
View Go Communicator Help
ews
nc files
nf files
rticles
nks
nembers
ome
THC-Secure Deletion 2.2
If you overwrite a file for 10+ times, it can *still* be recovered. Read why and use the programs included (w/src!). Written by van Hauser.
THC-Credit Version 1.9
World´s best Credit Card Generator, checks and generates over hundreds of different card types including newest bank ids and standarts. For all you horny guys who always wanted an account at Amateurs or Dirtybird, NOW supporting magnetic card reader and writer for MASTER/VISA/EC/etc cards.
THC-PBX Hacker Version 1.1
A tool to automatically hack any pbx, handles up to 10 different pbx numbers with features like random dialing, random dial/tone speed and length, completely programmable and much more. This will trick out any pattern detection switch.
THC-Login Hacker Version 1.1
Powerfull script language to hack terminal logins via dictionary- or bruteforce-hacking. Configurable for telnet and dialup hacking, extreme large command base.
THC-RA Hacking Kit #1
Backdoors, viris, traps and explainations for RemoteAccess BBS hacking. Sophisticated ways of getting hidden into BBS systems. Issue #1
THC-RA Hacking Kit #2
Document: Done

Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: http://www.2600.com/hacked_pages/2000/01/thomas.loc.gov/ What's Relate

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels RealPlayer

LmT and r00tcrew 0wN'z y0u! :-)

House Floor This Week | House Floor Now | Senate Schedule

LAMERS' TEAM

k1ck3r
null
shr1k3

equently Asked
uestions (FAQ's)

ample:
w to suck my d?ck)

Search CURRENT CONGRESS for XXX filez, movies, picz:

By Size By The Way Push IT! Clear

NEW This web site was change by the group LmT!

All goodies goes to k1ck3r, null, shr1k3 and AngelFire!!!

nT'z place:

ck3r
ll
r1k3
gelFire
prok

eets to r00t-cReW:

rkX
izmin
eib
UnDeR

r friends, who want to thax:

LEGISLATION | *CONGRESSIONAL RECORD* | COMMITTEE INFORMATION

Who are LmT?
We are 4 hackers from a little country in Europe! :]
You can reach us ..
k1ck3r

If you want to grow as individual you must first expand your mind.
null

-=# shr1k3 #=-
!@#$@$%^&%$ 1337
gr33tZ 2 a|| dud3Z r0ud m3!
shr1k3

I'd (k1ck3r) like to thanks to my girlfriend **Zlidka** and all the people which are around me and help me to live. **:-]**

And least we call our selves **LmT** and work together with **r00t-cReW**.

Special thanks to rage & p0||y .. da ozdrawiawash byrzo che ako znaesh kak shte izbuhnem na deepzone :)))))))))))

Document: Done

Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Stop

Bookmarks Location: http://www.2600.com/hacked_pages/2000/02/www.rsa.com/ What's Relate

Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels RealPlayer

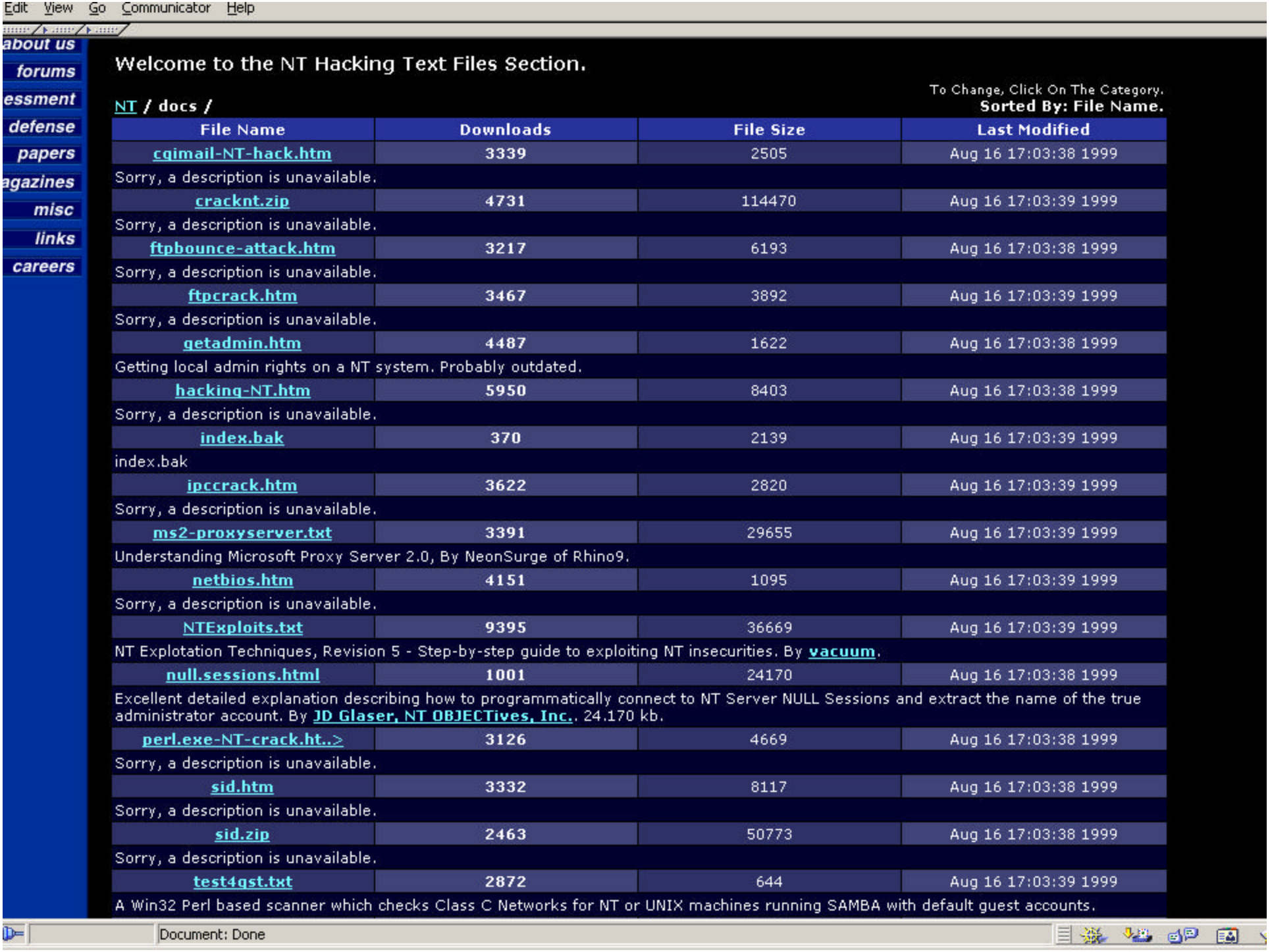
RSA ECURITY

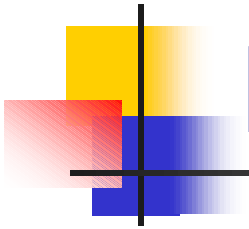
RSA Security inc. Hacked.
Trust us with your data! Praise Allah!

OWNED BY COOLIO

- Hello **aforce**!
- Girls are stupid and easy
- **RSA Laboratories Unveils Innovative** countermeasure to recent "Denial of Service" Hacker Attacks". Keep your data safe with us! Our security is the best.

Document: Done


Edit View Go Communicator Help
about us
forums
essment
defense
papers
agazines
misc
links
careers
Welcome to the NT Hacking Text Files Section.
To Change, Click On The Category.
Sorted By: File Name.
NT / docs /
File Name | Downloads | File Size | Last Modified
cgimail-NT-hack.htm | 3339 | 2505 | Aug 16 17:03:38 1999
Sorry, a description is unavailable.
cracknt.zip | 4731 | 114470 | Aug 16 17:03:39 1999
Sorry, a description is unavailable.
ftpbounce-attack.htm | 3217 | 6193 | Aug 16 17:03:38 1999
Sorry, a description is unavailable.
ftpcrack.htm | 3467 | 3892 | Aug 16 17:03:39 1999
Sorry, a description is unavailable.
getadmin.htm | 4487 | 1622 | Aug 16 17:03:38 1999
Getting local admin rights on a NT system. Probably outdated.
hacking-NT.htm | 5950 | 8403 | Aug 16 17:03:38 1999
Sorry, a description is unavailable.
index.bak | 370 | 2139 | Aug 16 17:03:39 1999
index.bak
ipccrack.htm | 3622 | 2820 | Aug 16 17:03:39 1999
Sorry, a description is unavailable.
ms2-proxyserver.txt | 3391 | 29655 | Aug 16 17:03:39 1999
Understanding Microsoft Proxy Server 2.0, By NeonSurge of Rhino9.
netbios.htm | 4151 | 1095 | Aug 16 17:03:39 1999
Sorry, a description is unavailable.
NTExploits.txt | 9395 | 36669 | Aug 16 17:03:39 1999
NT Explotation Techniques, Revision 5 - Step-by-step guide to exploiting NT insecurities. By vacuum.
null.sessions.html | 1001 | 24170 | Aug 16 17:03:38 1999
Excellent detailed explanation describing how to programmatically connect to NT Server NULL Sessions and extract the name of the true administrator account. By JD Glaser, NT OBJECTives, Inc.. 24.170 kb.
perl.exe-NT-crack.ht..> | 3126 | 4669 | Aug 16 17:03:38 1999
Sorry, a description is unavailable.
sid.htm | 3332 | 8117 | Aug 16 17:03:38 1999
Sorry, a description is unavailable.
sid.zip | 2463 | 50773 | Aug 16 17:03:38 1999
Sorry, a description is unavailable.
test4gst.txt | 2872 | 644 | Aug 16 17:03:39 1999
A Win32 Perl based scanner which checks Class C Networks for NT or UNIX machines running SAMBA with default guest accounts.
Document: Done

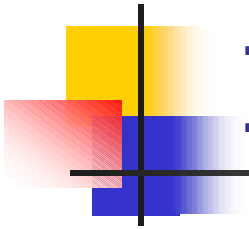


KaZaA

- KaZaA is another file sharing program that lets users download music, pictures, software, video clips and more.
- The fine print in the license agreement has something nasty.

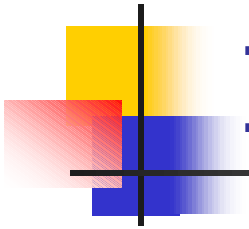
KaZaA License Agreement

- You hereby grant Brilliant Digital Entertainment the right to access and use the unused computing power and storage space on your computer/s and/or Internet access or bandwidth for the aggregation of content and use in distributed computing. The use acknowledges and authorizes this use without the right of compensation.



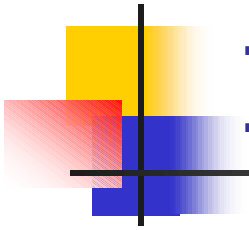
It Can't Happen Here

- 1984 – student sends obscene email to female faculty
- 1991 – Major Unix break-in, 18 machines, 5 depts, hackers from all over the world, discussed in the book @Large
- 1993 – Illegal music sites start to appear on VT systems
- 1995 – Student obtains test from faculty Mac ahead of time
- 1996 – Major relay attack, VT system used to attack other sites, AF-OSI/FBI involved



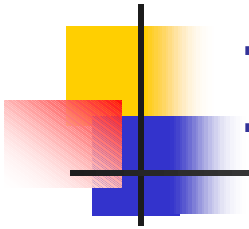
It Can't Happen Here

- 1996 – Student changes grades on instructor's PC
- 1996 – Anonymous email harassment from public VT systems
- 1996 – Hackers attack system in MCB, capture passwords from 3 depts
- 1996 – Secret Service investigates VT student for threat to the President via email
- 1996 – female instructor harassed via email on class listserv



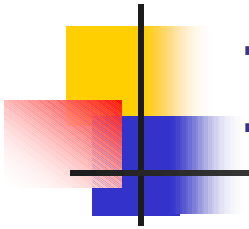
It Can't Happen Here

- 1996 – CO system attacked by BEV user
- 1996 – VT student captures 300 passwords in a dorm and changes them on 4/1/96
- 1997 – VT WWW site modified illegally
- 1997 – Dept. WWW sites attacked
- 1997 – VT student send hate mail to gay www site. VT Provost gets > 500 emails protesting this attack, story appears in NY Times, Washington Post, LA Times, CT, local PBS



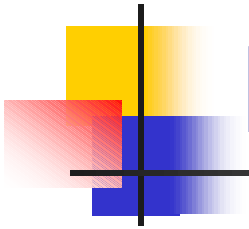
It Can't Happen Here

- 1997 – VT student sent to judicial review for email harassment & threats
- 1997 – Pirated software sites on VT systems
- 1997 – VT system attacked from outside, FBI involved
- 1997 – Hackers attack VT system to attack Canadian systems, RCMP/FBI involved
- 1998 – Hackers attack VT system to attack PSU systems
- 1998 – Dept lab attacked by disgruntled former grad student



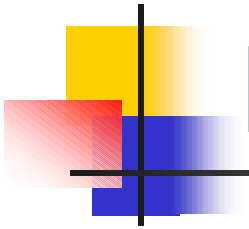
It Can't Happen Here

- 1998 – EE, Emporium labs attacked by hackers
- 1999 – BO, Netbus, Email attachment attacks arrive
- 1999 – +80 VT systems attacked to be used in DDOS attacks. FBI involved
- 2000 – Email harassment attacks continue
- 2000 – Remote control trojan attacks increase like VNC I showed you
- 2001 – VT systems continually probed for vulnerabilities

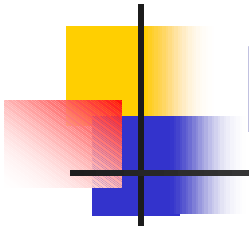


Four Initiatives To Fight Back

- Incident Response Team - sharing
- Education - sharing
- Policies – especial AUP
- STAR



Policies that Work

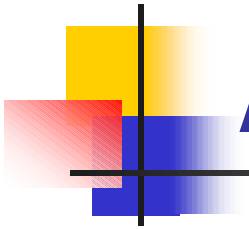


History

- 1989: I asked "Do we have a policy"
- 1990: first draft of the AUP
  - #2000 – adopted 1989, revised 1999
    - Management of University Records
  - #2005 – adopted 1989, revised 1999
    - Administrative Data Management and Access Policy
  - **#2015(AUP) – adopted 1991, revised 1999**
    - Acceptable Use Guidelines contain specific examples
  - #2020 – adopted 1991, removal pending
    - Policy on Protecting Electronic Access Privilege
  - #2030 – adopted 2000
    - Policy on Privacy Statements on VT WWW sites

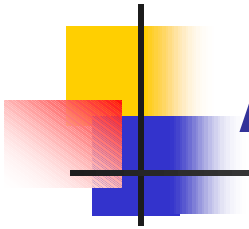
AUP Enforcement Philosophy

- Avoid repeating sanctions – they are in existing policies and sanctions
  - Sanctions are described in Student, Faculty and Staff Handbooks
  - Judicial procedure is defined there also
- Maintain compliance with Federal, state and local Computer Crime statutes.
  - Academic freedom vs. illegal activity



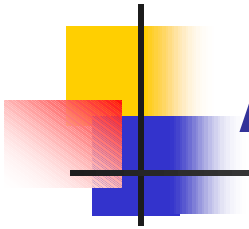
Acceptable Use Policy

- Scope
  - All VT-owned computer & communications facilities dealing with voice, video and data
  - VT Networks, mainframe, midrange, minicomputer, workstation and PC
  - No individually owned computers – until they connect to the VT network.



Acceptable Use Policy

- Demonstrates Respect of:
  - Privacy rights of others
  - Intellectual property rights (copyrights, patents)
  - **Data ownership**
  - Defense mechanisms
  - **Freedom from harassment, intimidation**



Acceptable Use – The Do's

- Use resources **for authorized purposes only**
  - Porno, personal business – violation!
- Responsibility
  - You're responsible for anything that originates from your system/userid.
- Permission
  - Access only what you've been given permission
    - You can share your userid/system but see previous point
  - Use only legal copyrighted software or data
- Refrain from overloading resources
  - Spam, DOS attacks

Acceptable Use – The DONT's

- Use another's system, userid, data, files or password without permission
- Use hacking programs, willfully spread viruses to break system security or disrupt services
- Make illegal copies of copyrighted materials, store them on VT systems or transmit them on VT networks
  - MP3, Napster, DVD is ok as long as copyrights are respected. (no music without permission)
  - You become a "distributor" – one kid who refused to eliminate all files brought up under judicial review and had a "suspended suspension."

Acceptable Use – The DON'Ts

- Use **email** or messaging services to **harass**, intimidate or threaten others
  - Most common offense
- Use VT systems for personal gain (your new startup company)
- Use VT systems for illegal purposes

Acceptable Use - Enforcement

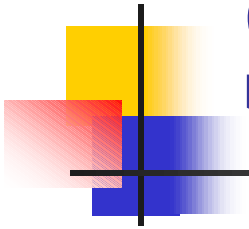
- AUP violations are a serious offense
- **VT reserves the right to copy and examine any file on VT systems allegedly related to AUP violations in order to protects its resources (no search warrant needed for VT system)**
  - Done only with the approval of supervisory or legal entities. Does NOT apply to personal systems
- FERPA, ECPA, Computer Fraud & Abuse Act, Computer Virus Eradication Act, VA Computer Crime Law, HIPPA, Interstate Transportation of Stolen Property Act

Acceptable Use - Statistics

- Students
  - 1998: 5 cases formally adjudicated
  - 1999: 1200 complaints, 25 cases formally adjudicated
  - Gender based harassment, copyright infringement pose significant contributory liability concerns for the University
  - Data from Office of Judicial Affairs annual report

Acceptable Use - Summary

- Comprehensive
- Flexible
- Use existing University Policies for enforcement
- Binding to all VT members
- Available at http://security.vt.edu, click on the Acceptable Use Guidelines



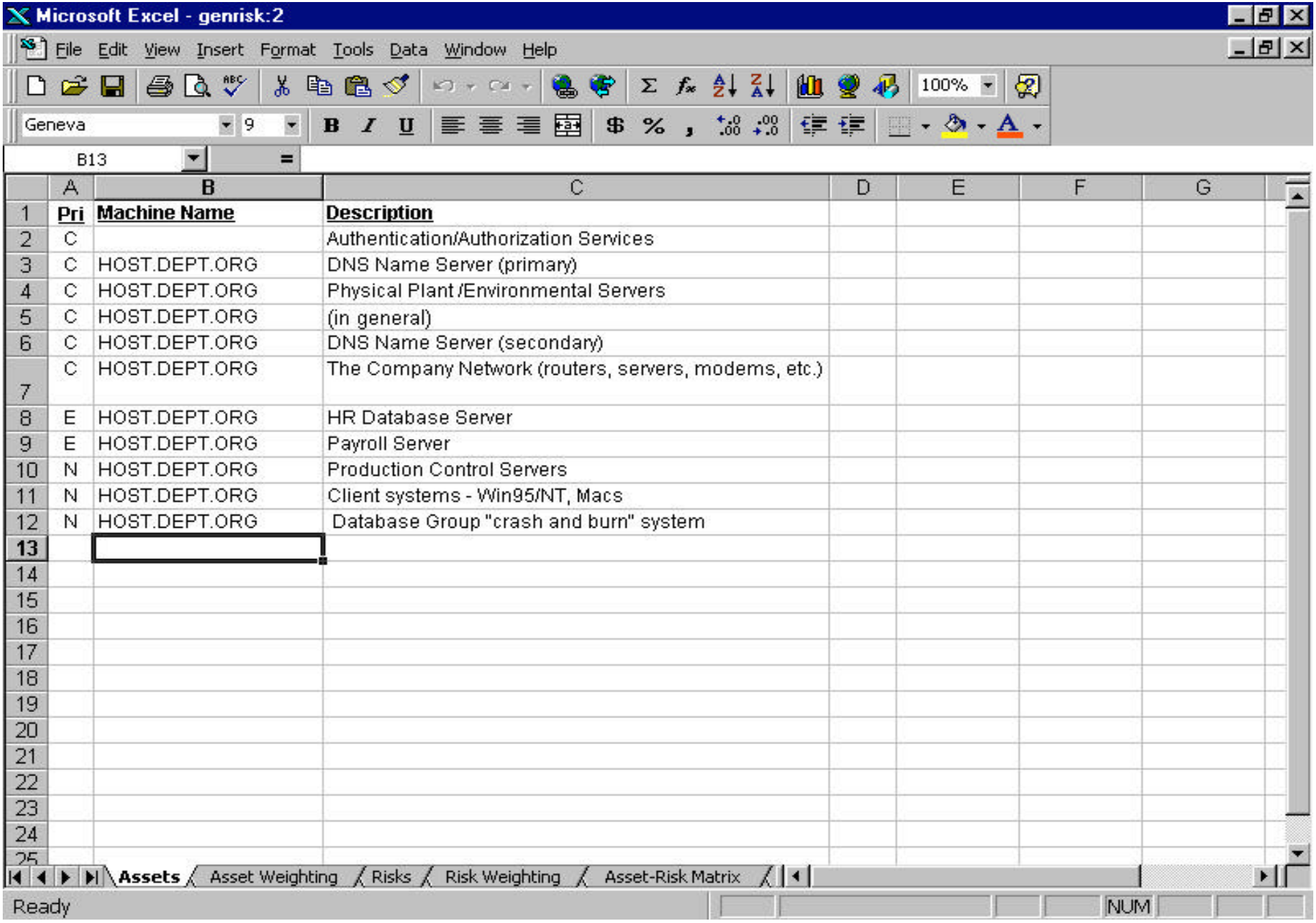
STAR

- How do you get the auditors, the security staff, and the systems administrators to all work together, and do it willingly?
- First make their jobs easier
- Then get senior management to require participation
- Get all three groups reading off the same page

STAR: Security Technology Assessment and Review

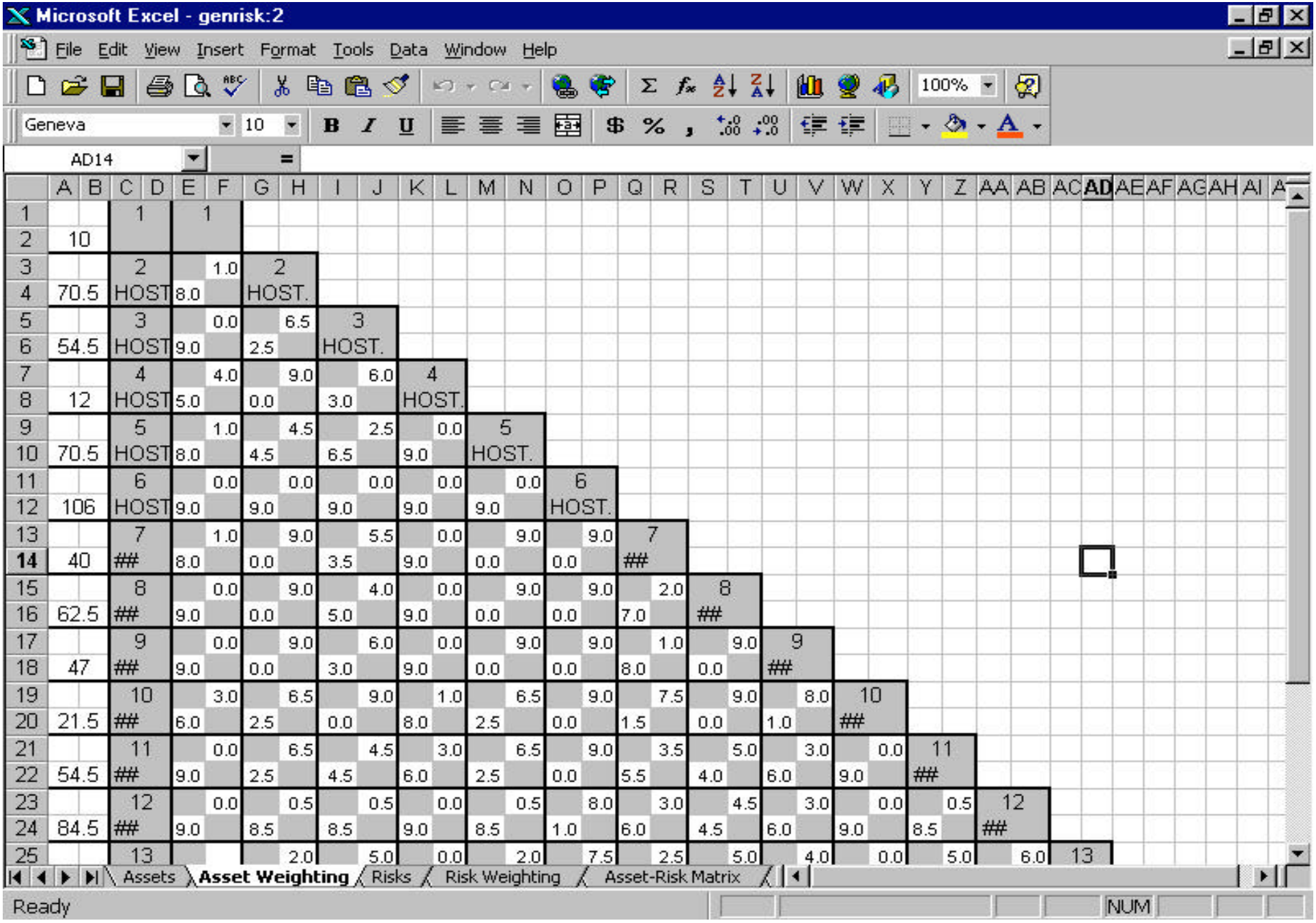
- Value your information assets
- Assess your risks
- Deploy risk-mitigating controls for maximum effect
- Create measures that drive human behavior

List your Assets

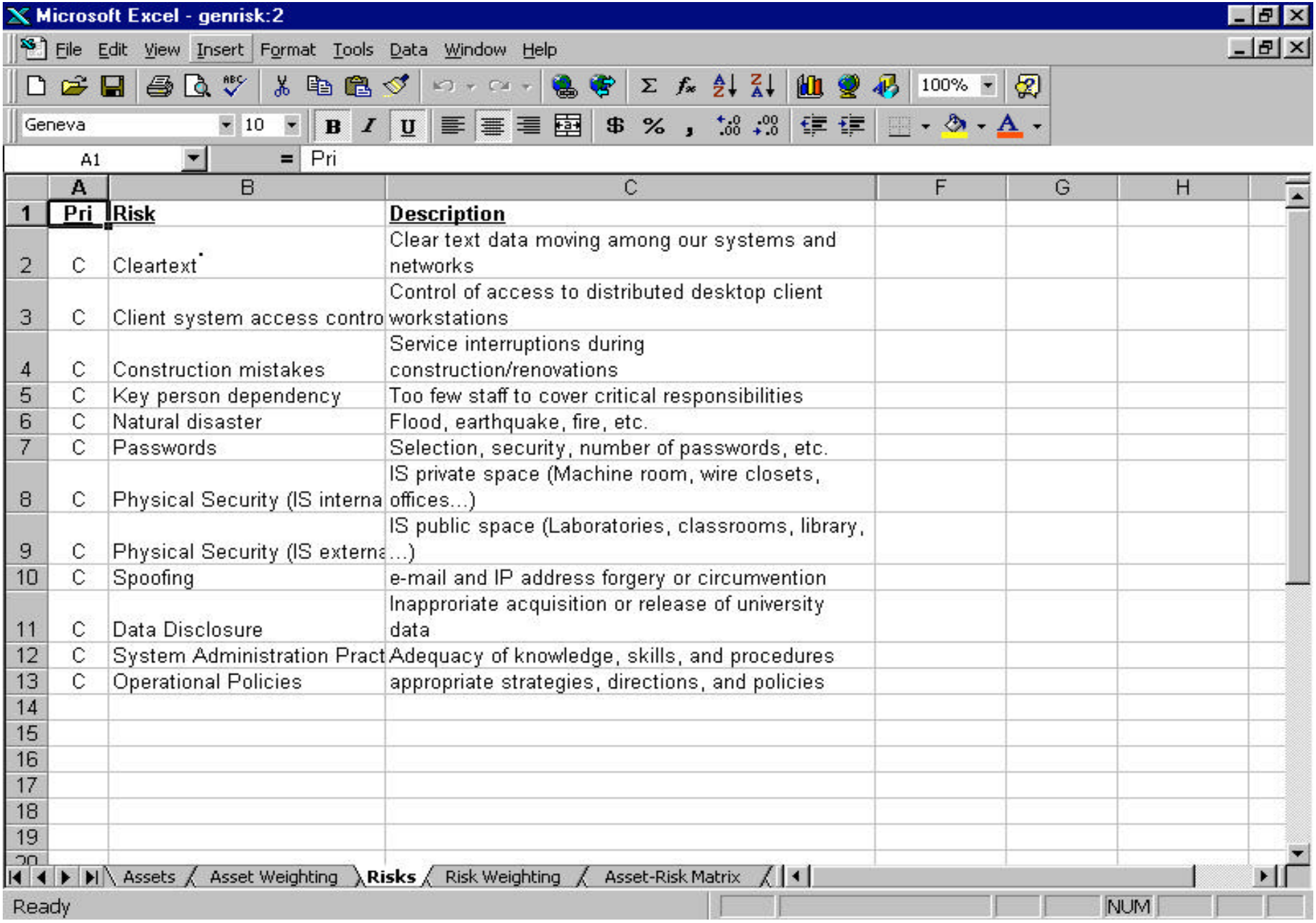


	A	B	C	D	E	F	G
1	**Pri**	**Machine Name**	**Description**				
2	C		Authentication/Authorization Services				
3	C	HOST.DEPT.ORG	DNS Name Server (primary)				
4	C	HOST.DEPT.ORG	Physical Plant /Environmental Servers				
5	C	HOST.DEPT.ORG	(in general)				
6	C	HOST.DEPT.ORG	DNS Name Server (secondary)				
7	C	HOST.DEPT.ORG	The Company Network (routers, servers, modems, etc.)				
8	E	HOST.DEPT.ORG	HR Database Server				
9	E	HOST.DEPT.ORG	Payroll Server				
10	N	HOST.DEPT.ORG	Production Control Servers				
11	N	HOST.DEPT.ORG	Client systems - Win95/NT, Macs				
12	N	HOST.DEPT.ORG	Database Group "crash and burn" system				
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							

Rank your Assets

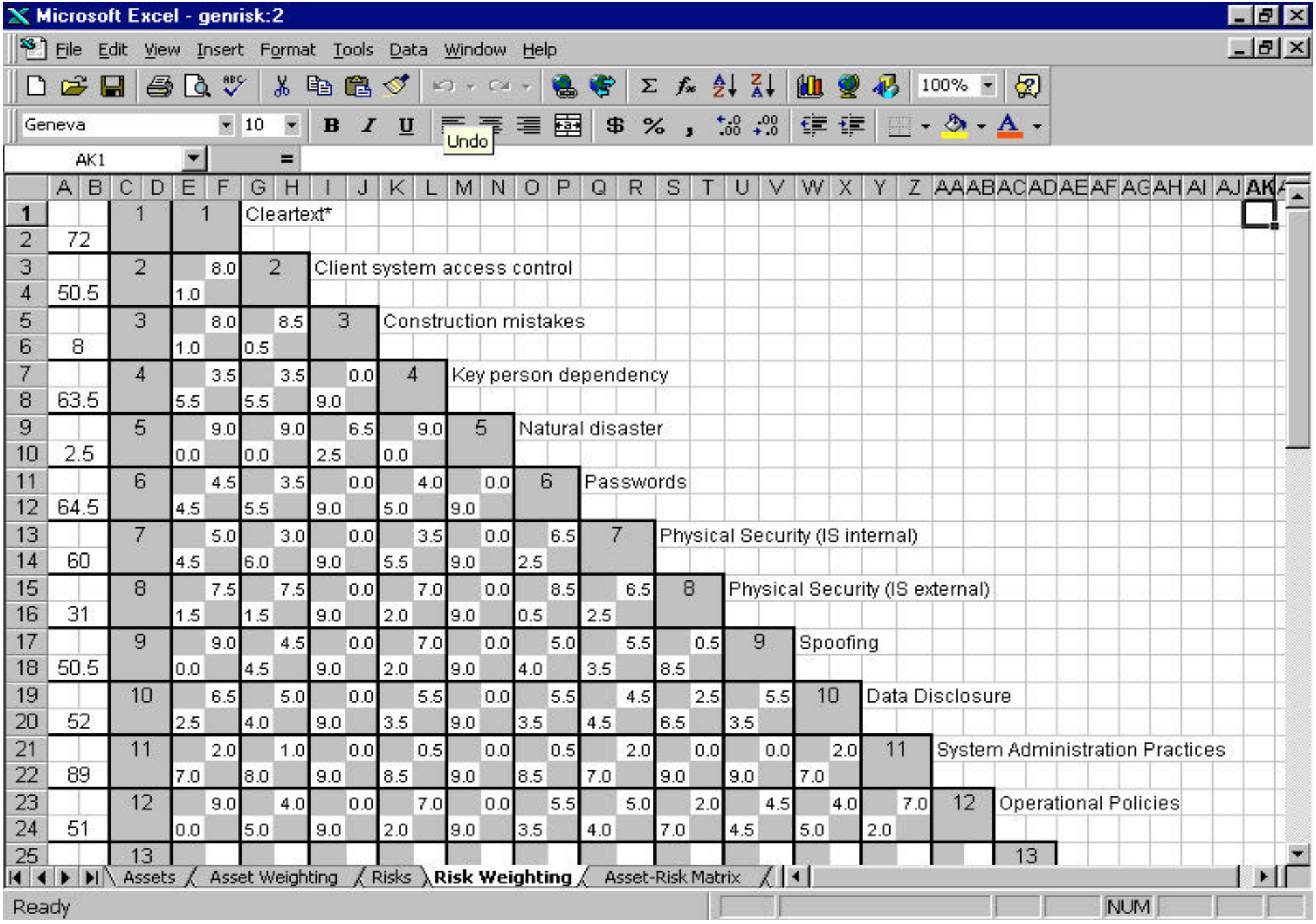


List your Risks

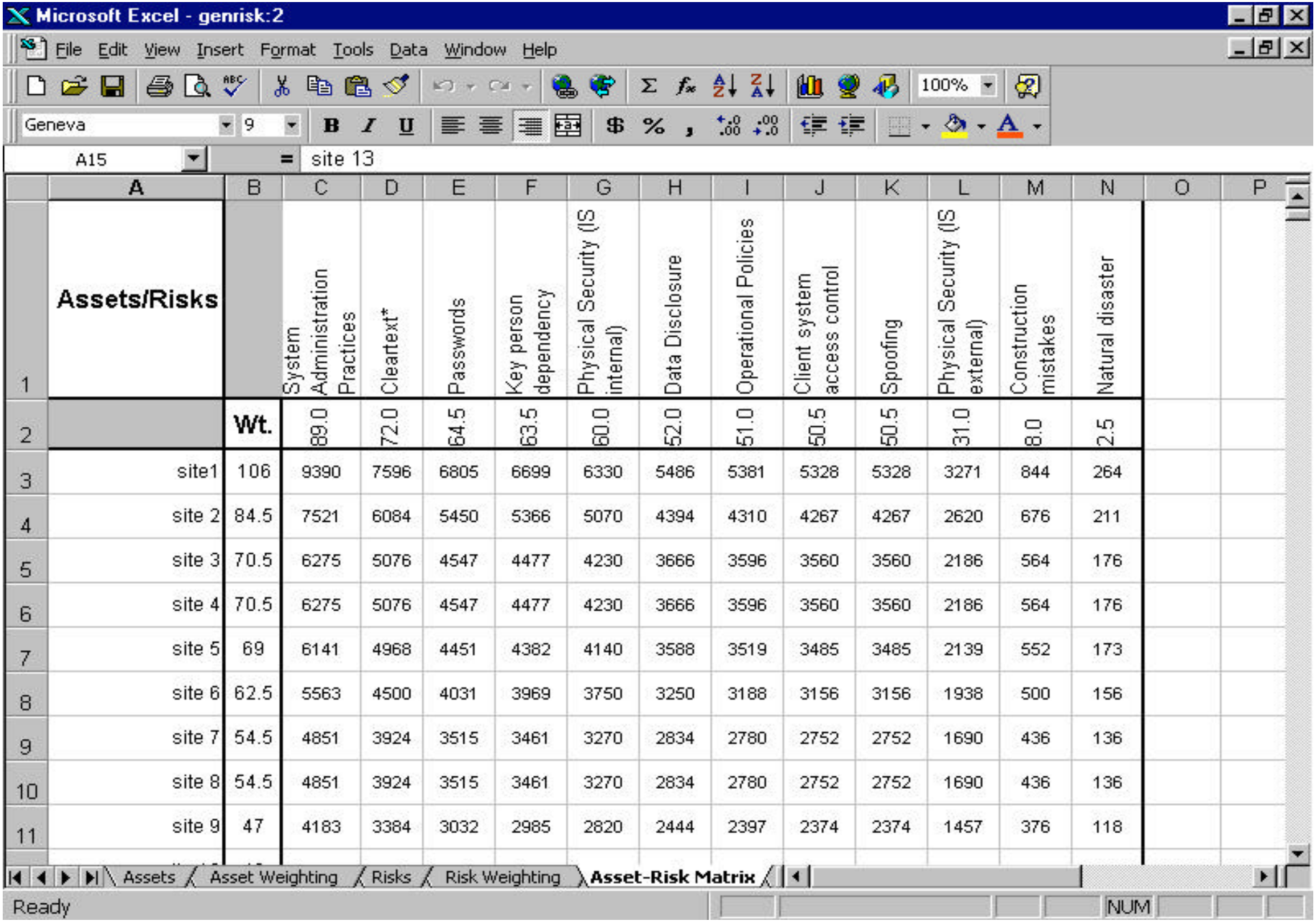


	A	B	C	F	G	H
1	**Pri**	**Risk**	**Description**			
2	C	Cleartext	Clear text data moving among our systems and networks			
3	C	Client system access contro	Control of access to distributed desktop client workstations			
4	C	Construction mistakes	Service interruptions during construction/renovations			
5	C	Key person dependency	Too few staff to cover critical responsibilities			
6	C	Natural disaster	Flood, earthquake, fire, etc.			
7	C	Passwords	Selection, security, number of passwords, etc.			
8	C	Physical Security (IS interna	IS private space (Machine room, wire closets, offices...)			
9	C	Physical Security (IS externa	IS public space (Laboratories, classrooms, library, ...)			
10	C	Spoofing	e-mail and IP address forgery or circumvention			
11	C	Data Disclosure	Inapproriate acquisition or release of university data			
12	C	System Administration Pract	Adequacy of knowledge, skills, and procedures			
13	C	Operational Policies	appropriate strategies, directions, and policies			
14						
15						
16						
17						
18						
19						
20						

Rank your Risks

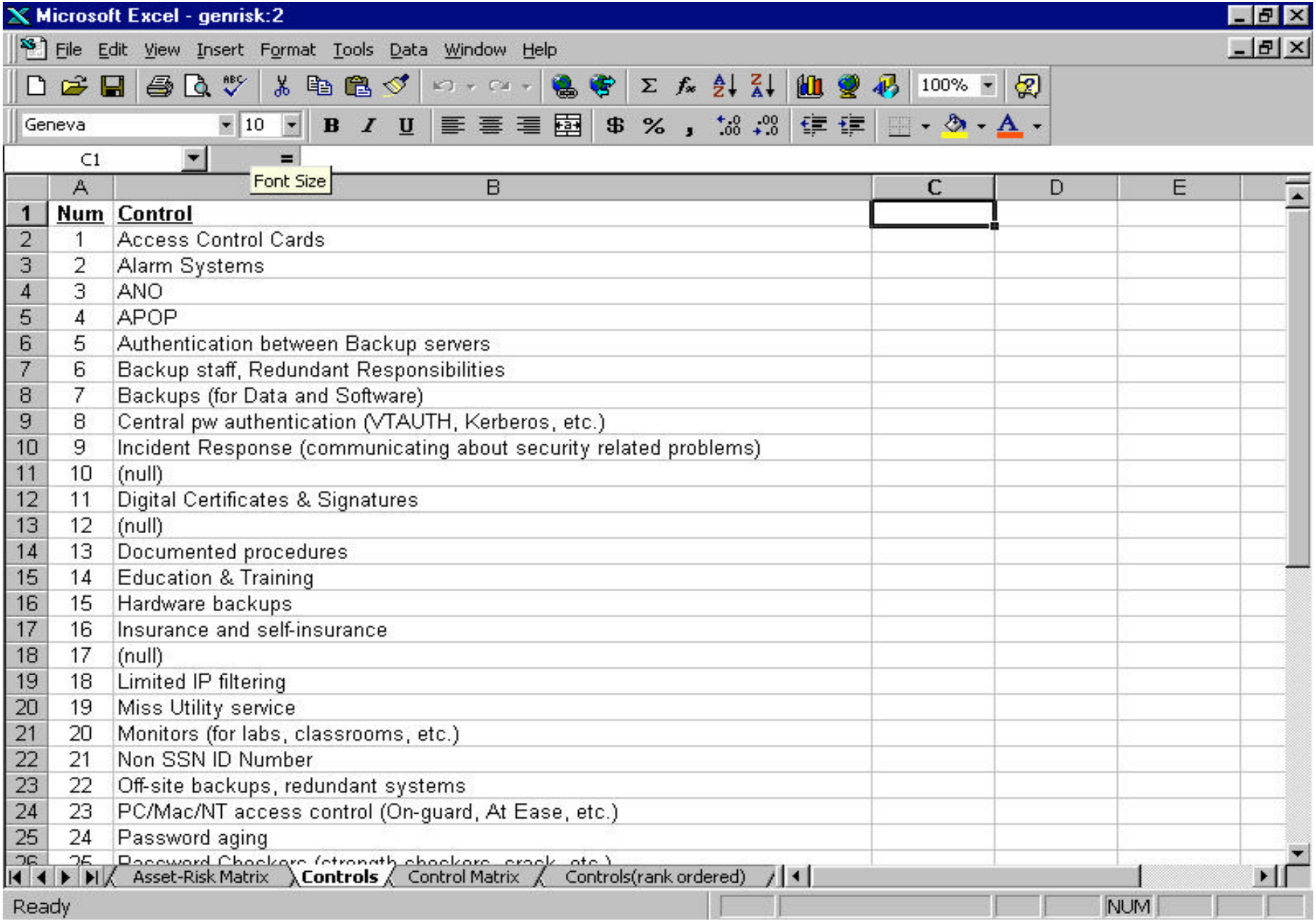


Map your Assets & Risks



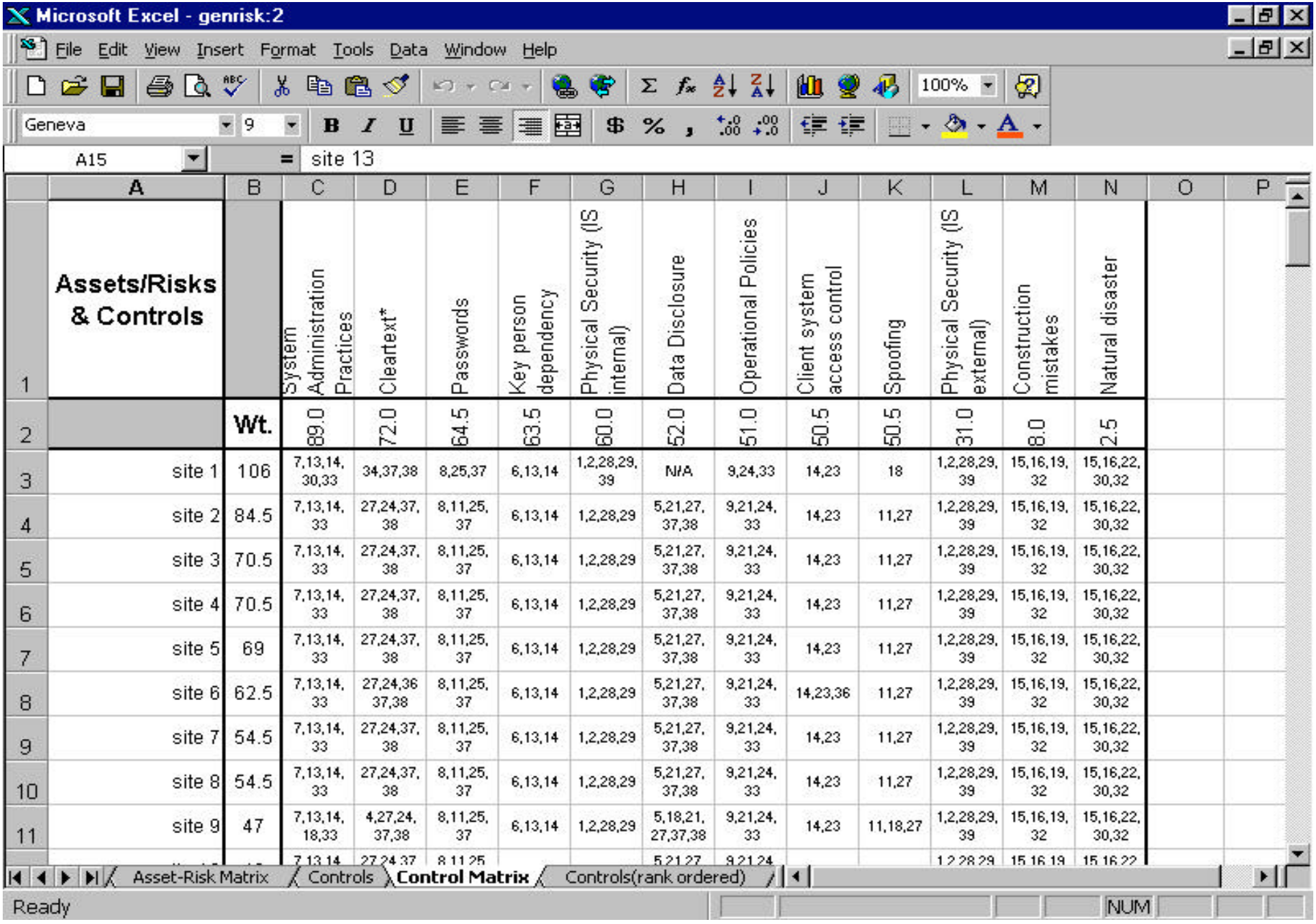
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	**Assets/Risks**		System Administration Practices	Cleartext*	Passwords	Key person dependency	Physical Security (IS internal)	Data Disclosure	Operational Policies	Client system access control	Spoofing	Physical Security (IS external)	Construction mistakes	Natural disaster		
2		**Wt.**	89.0	72.0	64.5	63.5	60.0	52.0	51.0	50.5	50.5	31.0	8.0	2.5		
3	site1	106	9390	7596	6805	6699	6330	5486	5381	5328	5328	3271	844	264		
4	site 2	84.5	7521	6084	5450	5366	5070	4394	4310	4267	4267	2620	676	211		
5	site 3	70.5	6275	5076	4547	4477	4230	3666	3596	3560	3560	2186	564	176		
6	site 4	70.5	6275	5076	4547	4477	4230	3666	3596	3560	3560	2186	564	176		
7	site 5	69	6141	4968	4451	4382	4140	3588	3519	3485	3485	2139	552	173		
8	site 6	62.5	5563	4500	4031	3969	3750	3250	3188	3156	3156	1938	500	156		
9	site 7	54.5	4851	3924	3515	3461	3270	2834	2780	2752	2752	1690	436	136		
10	site 8	54.5	4851	3924	3515	3461	3270	2834	2780	2752	2752	1690	436	136		
11	site 9	47	4183	3384	3032	2985	2820	2444	2397	2374	2374	1457	376	118		

List the Controls Available for Mitigating your Risks



Num	Control
1	Access Control Cards
2	Alarm Systems
3	ANO
4	APOP
5	Authentication between Backup servers
6	Backup staff, Redundant Responsibilities
7	Backups (for Data and Software)
8	Central pw authentication (VTAUTH, Kerberos, etc.)
9	Incident Response (communicating about security related problems)
10	(null)
11	Digital Certificates & Signatures
12	(null)
13	Documented procedures
14	Education & Training
15	Hardware backups
16	Insurance and self-insurance
17	(null)
18	Limited IP filtering
19	Miss Utility service
20	Monitors (for labs, classrooms, etc.)
21	Non SSN ID Number
22	Off-site backups, redundant systems
23	PC/Mac/NT access control (On-guard, At Ease, etc.)
24	Password aging
25	Password Checkers (strength checkers, crack, etc.)

Map your Controls onto your Assets & Risks



Microsoft Excel - genrisk:2

File Edit View Insert Format Tools Data Window Help

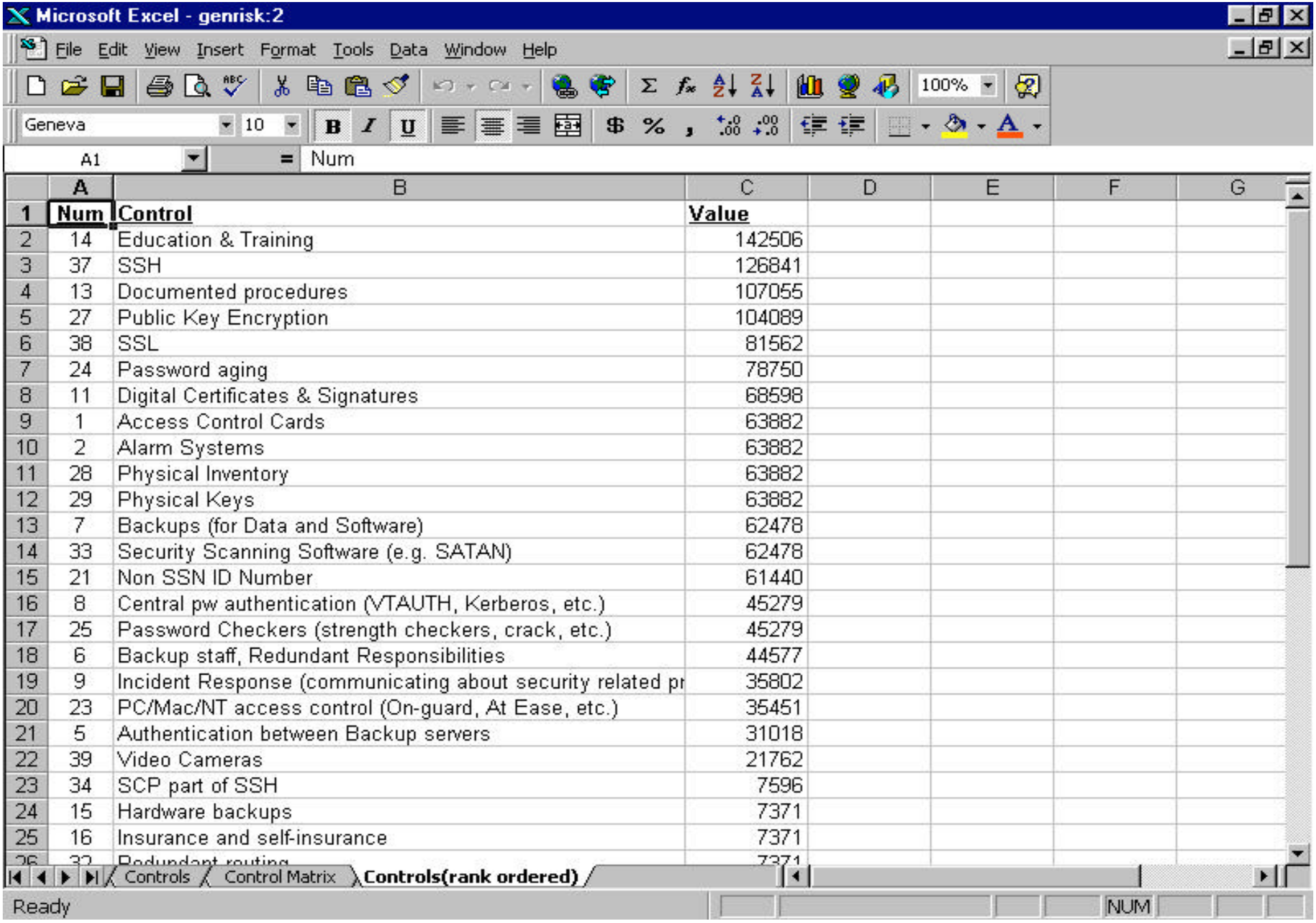
Geneva 9 — A15 = site 13

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	**Assets/Risks & Controls**		System Administration Practices	Cleartext*	Passwords	Key person dependency	Physical Security (IS internal)	Data Disclosure	Operational Policies	Client system access control	Spoofing	Physical Security (IS external)	Construction mistakes	Natural disaster		
2		**Wt.**	89.0	72.0	64.5	63.5	60.0	52.0	51.0	50.5	50.5	31.0	8.0	2.5		
3	site 1	106	7,13,14, 30,33	34,37,38	8,25,37	6,13,14	1,2,28,29, 39	N/A	9,24,33	14,23	18	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
4	site 2	84.5	7,13,14, 33	27,24,37, 38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
5	site 3	70.5	7,13,14, 33	27,24,37, 38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
6	site 4	70.5	7,13,14, 33	27,24,37, 38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
7	site 5	69	7,13,14, 33	27,24,37, 38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
8	site 6	62.5	7,13,14, 33	27,24,36 37,38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23,36	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
9	site 7	54.5	7,13,14, 33	27,24,37, 38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
10	site 8	54.5	7,13,14, 33	27,24,37, 38	8,11,25, 37	6,13,14	1,2,28,29	5,21,27, 37,38	9,21,24, 33	14,23	11,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		
11	site 9	47	7,13,14, 18,33	4,27,24, 37,38	8,11,25, 37	6,13,14	1,2,28,29	5,18,21, 27,37,38	9,21,24, 33	14,23	11,18,27	1,2,28,29, 39	15,16,19, 32	15,16,22, 30,32		

Asset-Risk Matrix | Controls | **Control Matrix** | Controls(rank ordered)

Ready NUM

Deploy your Controls for Maximum Effectiveness



Microsoft Excel - genrisk:2

File Edit View Insert Format Tools Data Window Help

Geneva 10

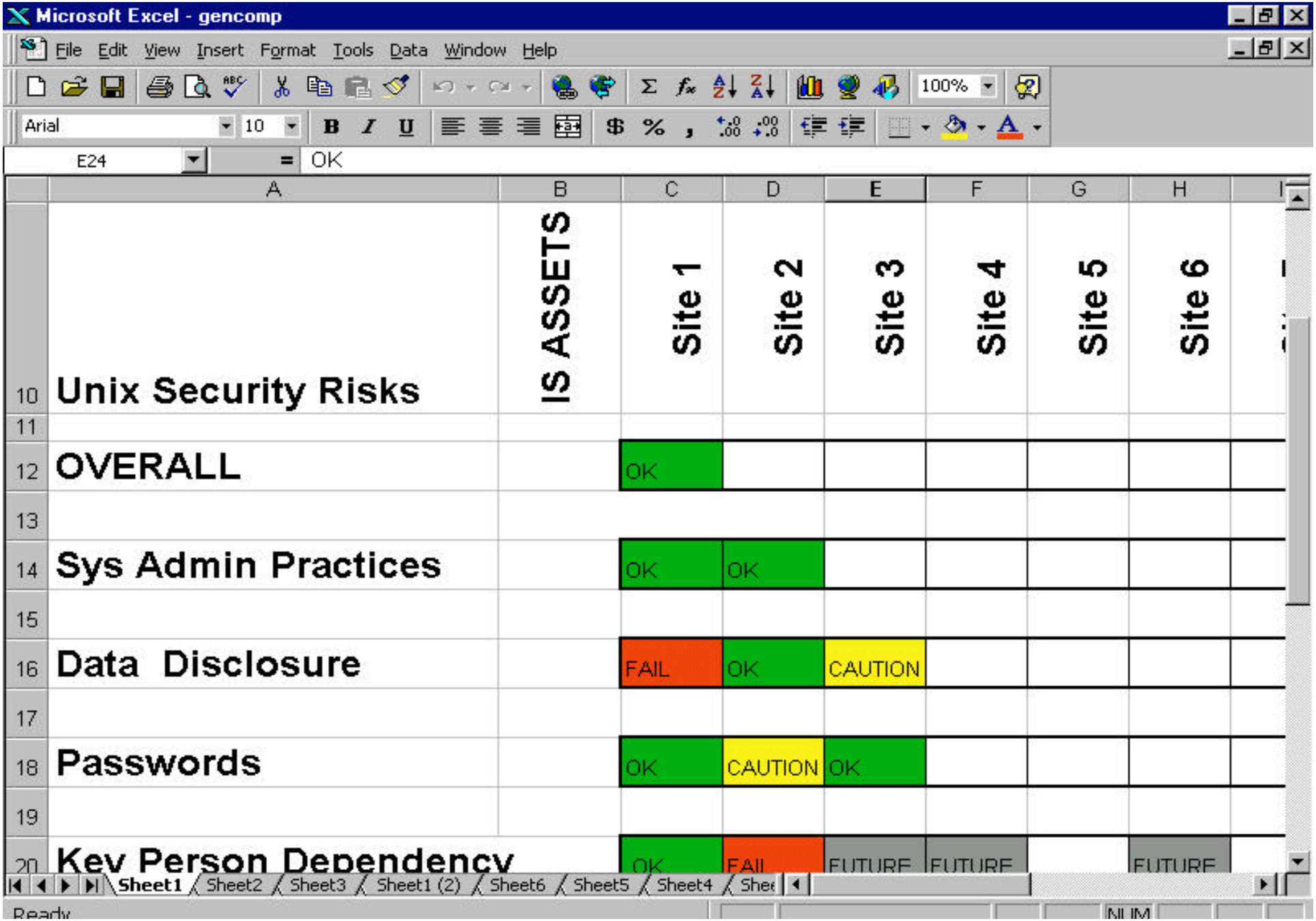
A1 = Num

	A	B	C	D	E	F	G
1	Num	Control	Value				
2	14	Education & Training	142506				
3	37	SSH	126841				
4	13	Documented procedures	107055				
5	27	Public Key Encryption	104089				
6	38	SSL	81562				
7	24	Password aging	78750				
8	11	Digital Certificates & Signatures	68598				
9	1	Access Control Cards	63882				
10	2	Alarm Systems	63882				
11	28	Physical Inventory	63882				
12	29	Physical Keys	63882				
13	7	Backups (for Data and Software)	62478				
14	33	Security Scanning Software (e.g. SATAN)	62478				
15	21	Non SSN ID Number	61440				
16	8	Central pw authentication (VTAUTH, Kerberos, etc.)	45279				
17	25	Password Checkers (strength checkers, crack, etc.)	45279				
18	6	Backup staff, Redundant Responsibilities	44577				
19	9	Incident Response (communicating about security related pr	35802				
20	23	PC/Mac/NT access control (On-guard, At Ease, etc.)	35451				
21	5	Authentication between Backup servers	31018				
22	39	Video Cameras	21762				
23	34	SCP part of SSH	7596				
24	15	Hardware backups	7371				
25	16	Insurance and self-insurance	7371				
26	32	Redundant routing	7371				

Controls | Control Matrix | Controls(rank ordered)

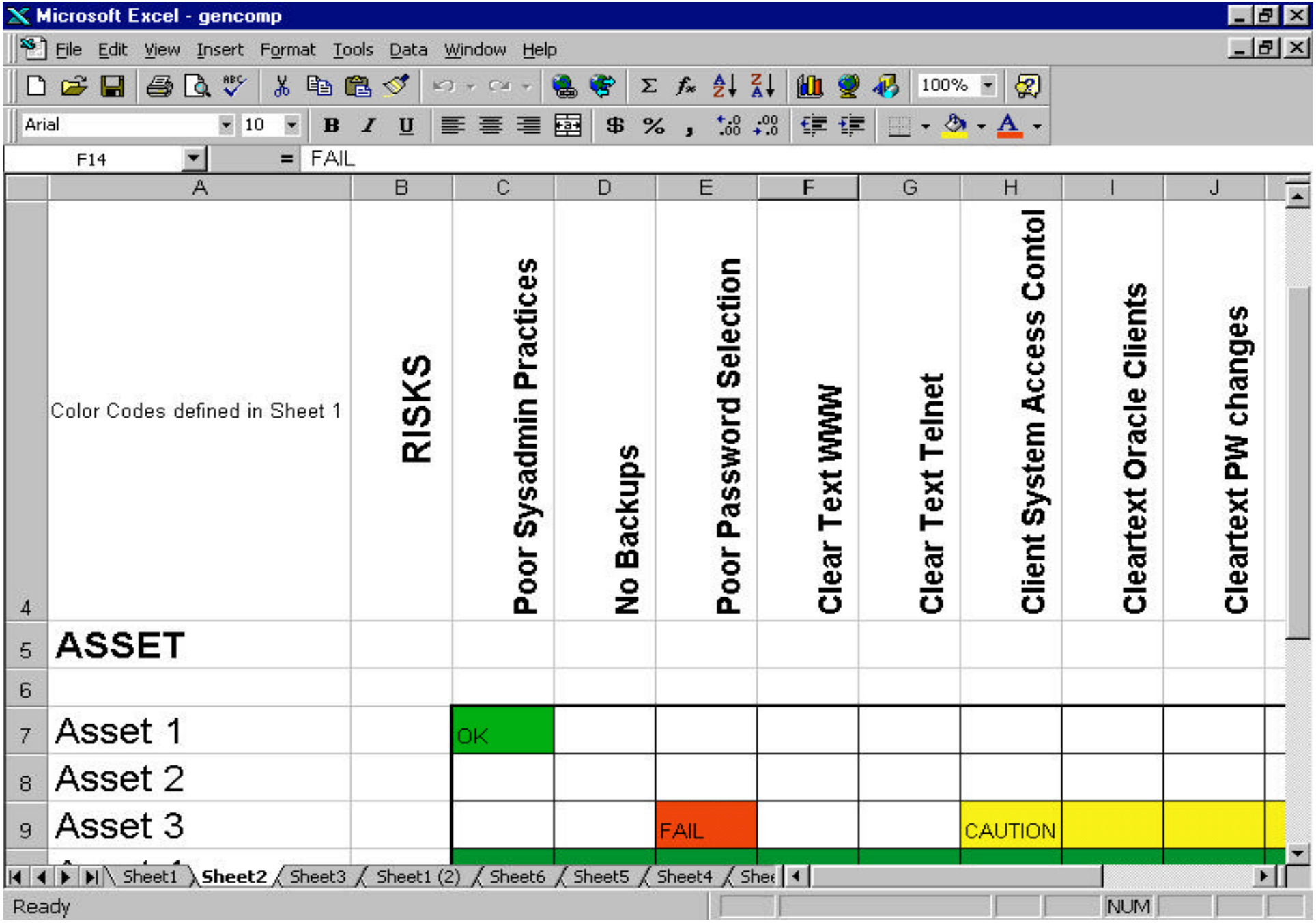
Ready NUM

Audit Compliance Status

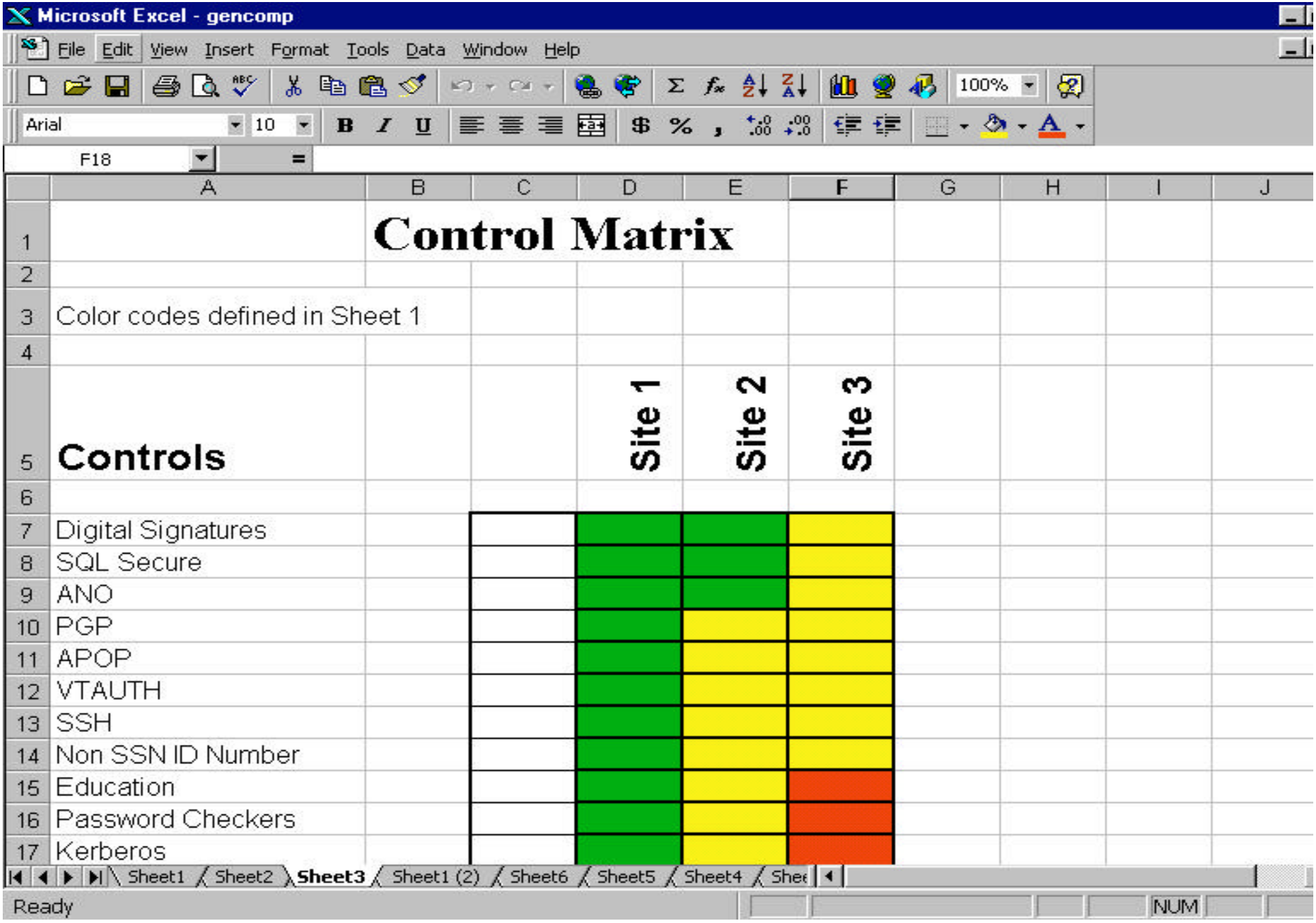


	A	B	C	D	E	F	G	H
10	Unix Security Risks	IS ASSETS	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6
11								
12	OVERALL		OK					
13								
14	Sys Admin Practices		OK	OK				
15								
16	Data Disclosure		FAIL	OK	CAUTION			
17								
18	Passwords		OK	CAUTION	OK			
19								
20	Key Person Dependency		OK	FAIL	FUTURE	FUTURE		FUTURE

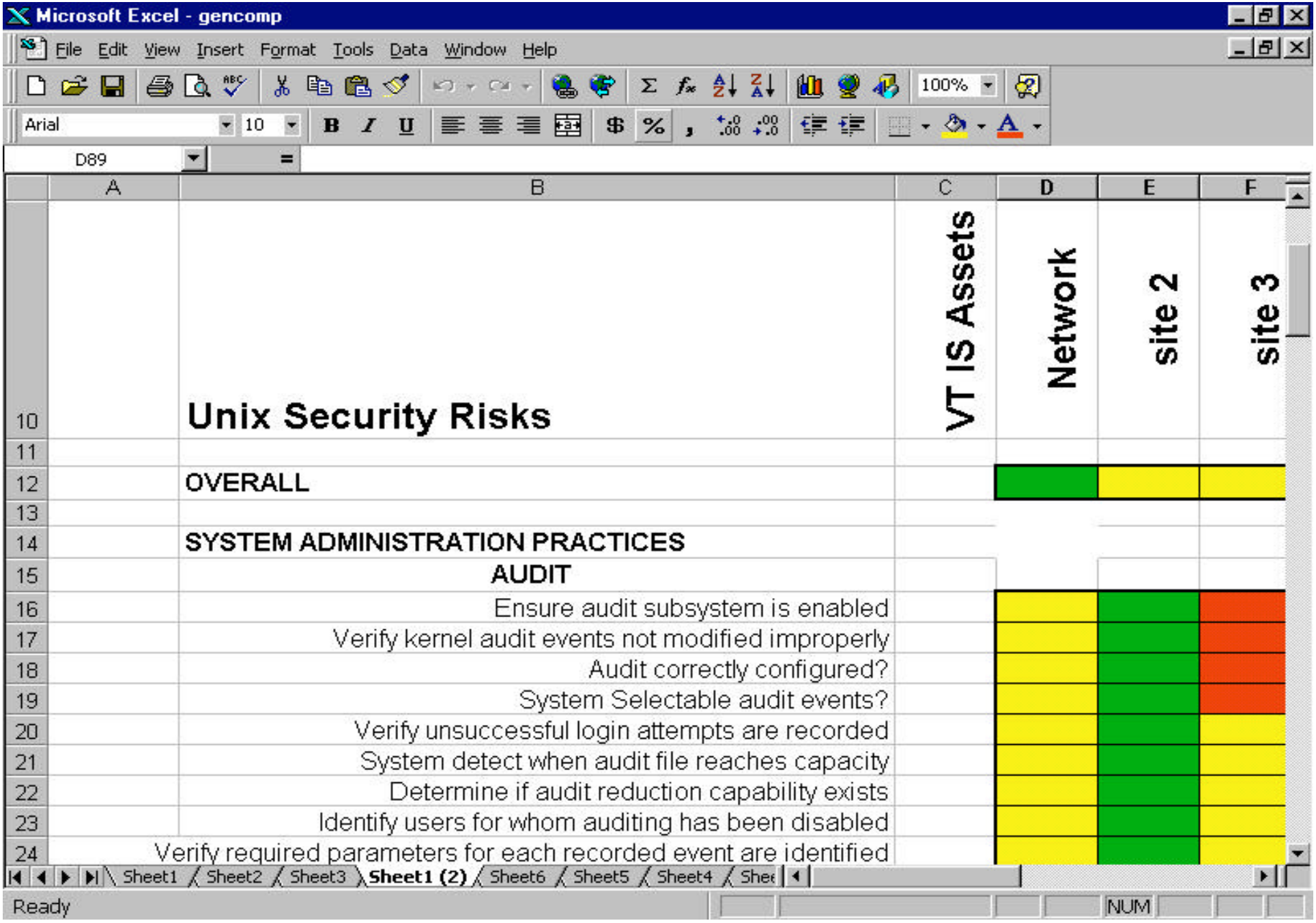
Assets/Risks Status



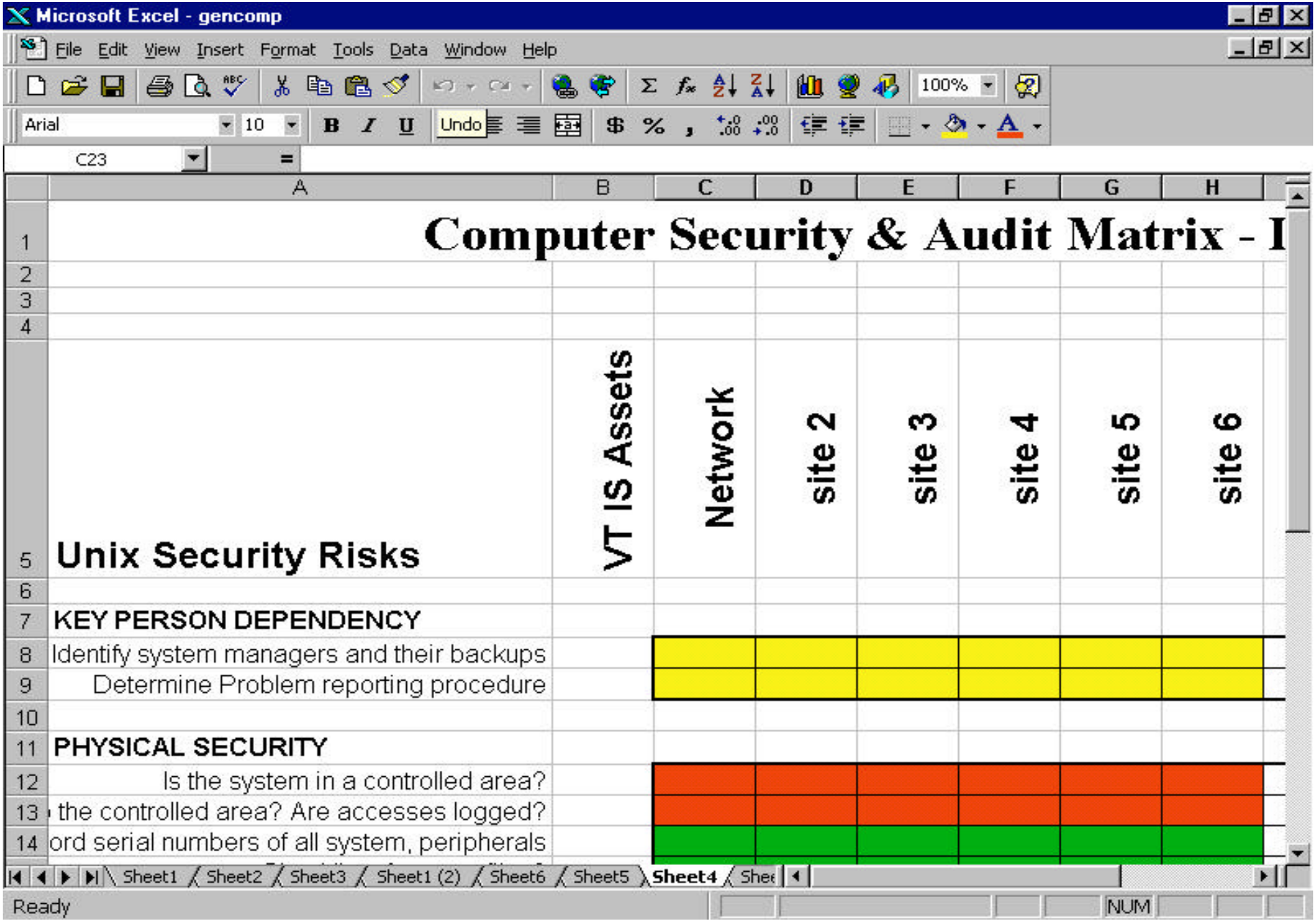
Controls Status by Asset

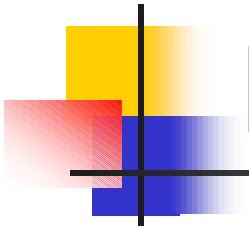


Detailed Audit Compliance Status



Detailed Audit Compliance Status





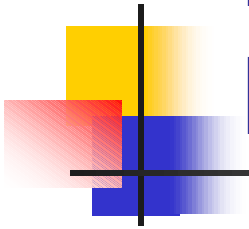
Benefits to User Organizations

- List of risks they hadn’t considered
- List of assets that are at risk
- List of controls – possible solutions
- Decision-making process is up to them

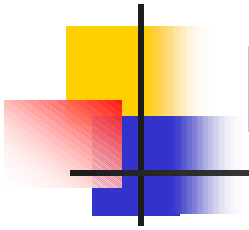
Benefits to Auditors

- Amount of work reduced in 2nd year and beyond
- Consistent reports
- Comparisons and trend analysis

Benefits to Incident Response People



- Do not get auditor information
- But, if problem occurs, can get good picture of what controls were on which machine



Benefits To System Managers

- Provides answer to management of “Where are we now and what do we need to do to get to a reasonable level”
- New: using Center for Internet Security scoring tools – because that catches management’s eyes.
- Once they saw the scores (1-10) they demanded action.
- Auditor’s like it, too.

New Additions at the Web Site

- Business Impact Analysis/Risk Assessment Template
- Emergency Response Plan

File Edit View Go

Member: guest | Sign In | Member Services | Help | Internet @ Home

Mail Search Bookmarks | excite | MyExcite News Shopping People Shortcuts | Nashville Area | Local Media Sports Community Arts

Excite Home | http://security.vt.edu/ | go | security.vt.edu

computing | answers | pidtool | software | banner | security | Virginia Tech

SECURITY.VT.EDU

Home | Help

You Are Here: security.vt.edu

Know The Rules

It is a good idea to familiarize yourself with the rules and regulations that govern your use of computers and other systems.

- Report A Violation
- University Policies
- State & Federal Organizations
- Special Interest Organizations

Play It Safe

The best way to protect yourself is to not put yourself into situations that put you or your data at risk. These tools allow you to analyze your risk and take preventative measures.

- Protective Software
- Business Recovery Plan
- Risk Analysis (STAR)
- Backup Services

Lock It Down

By securing your system, you make it harder for would-be attackers to invade your machine. The software, tools, and

Go To Class

The best way to protect yourself from attacks is to educate yourself. Virginia Tech and other groups in our area

Acceptable Use Policy
All users of the Virginia Tech network must abide by this policy.

Report a Violation
Send an e-mail to the Office of Judicial Affairs.

Security News

- Security hole in Java may expose servers
- BUGS 4.0.1
- Advanced Directory Printer
- OutGuess
- The Microsoft Web Outage: What Went Wrong? (article)

Provided by Security Focus

Other Security Sites

search

Questions?